TABLE OF CONTENTS

SECTION **PAGE**

LIST OF TABLES

TABLE **PAGE**

Changes to UCR 2010, Section 5.3.5, IPv6 Requirements

SECTION	CORRECTION	EFFECTIVE DATE
5.3.5.1	Description of relationship between DISR Version 5.0 and the UCR 2010 is added with differences between the two documents defined.	No action required
5.3.5.2	New definitions and material added to define the system characteristics for UCR 2010.	No action required
5.3.5.3	New IPv6 Rules of Engagement (RoE) for UCR 2010	Immediately
5.3.5.4	Add requirement 1.4 on seamless transition from IPv4 to IPv6 for functions	Immediately
5.3.5.4.4	Add note to Requirement 10 on how address registration is to be done.	Immediately
5.3.5.4.5	Requirement 11 delete RFC 2461	Immediately
5.3.5.4.5	Requirement 11 make RFC 4861 effective for UCR 2010	Immediately
5.3.5.4.5	Requirement 11.1 Delete note	Immediately
5.3.5.4.5.1	Requirement 11.7.1 Delete requirement for EBC Redirect	Immediately
5.3.5.4.5.1	Requirement 11.7.2 Delete requirement for EBC Redirect	Immediately

SECTION	CORRECTION	EFFECTIVE DATE
5.3.5.4.5.1	Add Requirement 11.7.3 for a device to disable redirect.	Immediately
5.3.5.4.6	Requirement 12 delete RFC 2462	Immediately
5.3.5.4.6	Requirement 11 make RFC 4862 effective for UCR 2010	Immediately
5.3.5.4.6	Clarification provided for Requirement 12.1	Immediately
5.3.5.4.6	Clarification provided for Requirement 12.1.1 including a summary table of addressing methods	Immediately
5.3.5.4.6	Clarification provided for Requirement 12.2 with respect to DAD	Immediately
5.3.5.4.6	Clarification provided for Requirement 12.2.1 with respect to allowable conditions for disabling DAD	Immediately
5.3.5.4.6	Requirement 12 delete RFC 3041	Immediately
5.3.5.4.6	Requirement 12 make RFC 4941 effective for UCR 2010	Immediately
5.3.5.4.7	Requirement 14: Make RFC 4443 Required for LS	Immediately
5.3.5.4.7	Requirement 14.2: Make RFC 4443 Required for Destination Unreachable	
5.3.5.4.7	Requirement 14,2 Add note to provide an alternative to Paragraph 3.1 of RFC 4443.	Immediately
5.3.5.4.7	Requirement 14.3 Echo reply Required for LS	Immediately
5.3.5.4.8	Requirement 15 delete RFC 2740	Immediately
5.3.5.4.8	Requirement 15 make RFC 5340 effective for UCR 2010	Immediately
5.3.5.4.8	Requirement 15.3 add note about tactical environment.	No action required.
5.3.5.4.8	Requirement 15.4 Add Requirement for RFC 5838 for UCR 2012	No action required.
5.3.5.4.8	Requirement 15a Make RFC 5308 effective for UCR 2010.	Immediately
5.3.5.4.8	Requirement 15a.1 Make RFC 5304 effective for UCR 2010.	Immediately
5.3.5.4.8	Requirement 15a.1 Make RFC 5310 effective for UCR 2010.	Immediately
5.3.5.4.8	Requirement 17 delete RFC 2858	Immediately
5.3.5.4.8	Requirement 17 make RFC 4760 effective for UCR 2010	Immediately
5.3.5.4.9	Requirement 17 delete RFC 2401	Immediately
5.3.5.4.9	Requirement 17 make RFC 4301 effective for UCR 2010	Immediately
5.3.5.4.9	Requirement 22.13.2 is effective for UCR 2010	Immediately

SECTION	CORRECTION	EFFECTIVE DATE
5.3.5.4.9	Requirement 22.14 RFC 2409 is effective for UCR 2012	No action required
5.3.5.4.9	Requirement 22.14 RFC 4306 is effective for UCR 2012	No action required
5.3.5.4.9	Requirement 22.14.11 RFC 4308 is effective for UCR 2012	No action required
5.3.5.4.9	Requirement 22.14.12 RFC 4869 is effective for UCR 2012	No action required
5.3.5.4.9	Requirement 22.19 delete RFC 4305	Immediately
5.3.5.4.9	Requirement 22.19 make RFC 4835 effective for UCR 2010	Immediately
5.3.5.4.10	Requirement 29 RFC 4295 is effective for UCR 2012	No action required
5.3.5.4.10	Requirement 30 Delete RFC 3595	Immediately
5.3.5.4.13	Requirement 42 delete RFC 3266	Immediately
5.3.5.4.13	Requirement 42 make RFC 4566 effective for UCR 2010	Immediately
5.3.5.4.14	Requirement 48 RFC 3775 is effective for UCR 2012	No action required
5.3.5.4.14	Requirement 48.1 RFC 3775 is effective for UCR 2012	No action required
5.3.5.4.14	Requirement 49 RFC 3776 is effective for UCR 2012	No action required
5.3.5.4.14	Requirement 49 RFC 4877 is effective for UCR 2012	No action required
5.3.5.4.14	(new) Requirement 50 RFC 4429 is effective for UCR 2012	No action required
5.3.5.4.14	(new) Requirement 50 RFC 3971 is effective for UCR 2012	No action required
5.3.5.4.14	Requirement 51 RFC 3963 is effective for UCR 2012	No action required
5.3.5.4.14	(new) Requirement 52.1 RFC 3168 is effective for UCR 2010	18 Month Rule
5.3.5.4.14	Requirement 55 delete RFC 2472	Immediately
5.3.5.4.14	Requirement 55 make RFC 5072 effective for UCR 2010	Immediately
5.3.5.4.14	(new) Requirement 56 RFC 5798 is effective for UCR 2010	18 Month Rule
5.3.5.4.14	(new) Requirement 57 RFC 4330 is effective for UCR 2012	No action required
5.3.5.4.14	(new) Requirement 58 ROHC RFCs may be included in UCR 2012	No action required
5.3.5.4.14	(new) Requirement 59 Header Compression RFCs may be included in UCR 2012	No action required
5.3.5.4.14	(new) Requirement 60 Multicast RFCs may be included in UCR 2012	No action required

SECTION	CORRECTION	EFFECTIVE DATE
5.3.5.5	Table 5.3.5-2	Various
5.3.5.5	Table 5.3.5-3	Various
5.3.5.5	Table 5.3.5-4	Various
5.3.5.5	Table 5.3.5-5 (Table divided into three parts)	Various
5.3.5.5	Table 5.3.5-6	Various

5.3.5 IPv6 Requirements

~~Section 5.3.5 describes the IPv6 requirements for SBU UC subsets provided by the DSN, DVS, circuit emulation, and/or short, latency sensitive C2 messages.~~ Section 5.3.5 describes the IPv6 requirements for Sensitive But Unclassified (SBU) Unified Capabilities subsets provided by all products and technologies used to send and receive or to support voice, video, or data across DoD networks that provide UC services.

5.3.5.1 Introduction

The DISR baseline is updated to ensure that DoD Capabilities for building and buying IT products are based on a current and effective set of IT NSS standards. "DoD IPv6 Standard Profiles for IPv6-Capable Products" Version 5~~3~~.0 (Ref: DoD memorandum, sub: Department of Defense IT Standards Registry Baseline Release 08-2.0, dated July 26~~14~~, 2010~~08~~.) is approved for distribution via the DISR for IPv6 for DoD IT equipments, including those for UC, providing a seamless integration of voice, video, and data applications. ~~However, version 4.0 of the "DoD IPv6 Standard Profiles for IPv6-Capable Products" has been approved (Ref: DoD memorandum, sub: Department of Defense IT Standards Registry Baseline Release 09-2.0, dated July 30, 2009) and has already deprecated version 3.0. Unless specifically addressed in this section, all UCR products shall comply with version 4.0 of the "DoD IPv6 Standard Profiles for IPv6-Capable Products".~~

"DoD IPv6 Standard Profiles for IPv6-Capable Products" version 5~~4~~.0 is included at the end of Section 5.3.5.

~~The sole exemption at this time is the VVoIP products defined in this section. The VVoIP products addressed by this exemption are defined in table 5.3.5-1 and the associated IPv6 requirements are based on the DoD IPv6 Profile, Version 3.0, with five exceptions as follows:~~

~~1. If the DoD IPv6 Profile, Version 4.0, has identified an Information Assurance risk that must be mitigated with a new requirement.~~

~~2. If the DoD IPv6 Profile, Version 4.0, has deleted a requirement, which is cited in Version 3.0.~~

~~3. If the DoD IPv6 Profile, Version 3.0, cites an RFC with SHOULD for the product class while the UCR cites a REQUIRED in this case.~~

~~4. If there is a UCR unique requirement that is levied on the UCR product and is not included in the DoD IPv6 Profile.~~

~~5. If the DoD IPv6 Profile, Version 3.0, cites a mandatory requirement for an RFC and the UCR cites a conditional requirement for the same RFC.~~

~~In Tables 5.3.5-2 to 5.3.5-6, these exceptions are identified with an asterisk (*(n)) where *n* is one of these five exceptions.~~

~~In some cases, DoD IPv6 Profile, Version 3.0, will identify RFCs which will be deprecated. For example, in DoD IPv6 Profile, Version 4.0, RFC 2740 "Open Shortest Path First (OSPF) for IPv6," will be superseded by RFC 5340 in 2010. In the text of UCR 2010, this case is denoted by: "RFC 2740 and RFC 5340 (UCR 2010)." This is to be interpreted to mean that:~~

~~1. Under UCR 2010, the use of either RFC 2740 or RFC 5340 is acceptable.~~

~~2. Under UCR 2010, the requirement for RFC 5340 will be mandatory.~~

~~Also, UCR 2010, includes some specific subtended requirements to the underlining RFCs for reasons of Information Assurance or Interoperability~~

If there are differences between this UCR and the "DoD IPv6 Standard Profiles for IPv6-Capable Products," Version 5~~3~~.0, the UCR takes precedence over the DoD IPv6 Profile, version 5~~3~~.0. However, for any appliance that is not defined in the UCR 2010, the vendor is to follow DoD IPv6 Profile version 5~~4~~.0.

The DoD IPv6 Profile includes Network Appliance and Simple Server, and notes that the distinction between them results in no real difference in requirements or testing. Hence, the product class is identified as "Net App or Simple Server." UCR ~~2010,~~ will follow the DoD IPv6 Profile guidance and identify the product class as "NS/SS."

For the DoD IPv6 Profile, Information Assurance devices include firewall, IDS, authentication server, security gateway, HAIPE, and VPN concentrator. The UC IPv6 requirements for an EBC are specified in the UCR. Guidance for UC IPv6 requirements for Intrusion Protection System (IPS), IDS, firewall, and VPN can be found in DoD IPv6 Profile, Version ~~4~~5.0.

5.3.5.2 Characteristics

The system requirements specified in Section 5.3.2, Assured Services Requirements, are the minimum set of requirements necessary for the system to be IPv6-capable for Video and Voice over IP (VVoIP). An implementer may choose to specify additional IPv6 requirements based on its non-VVoIP or unique VVoIP requirements. Also, a vendor may choose to implement additional IPv6 functions based on its commercial market. This section focuses on the deltas between an IPv6 implementation and an IPv4 implementation, and does not address

consistencies or inconsistencies between IPv4 and IPv6. ~~The requirements are CY 2009 requirements unless specifically stated that the requirement applies to a different timeframe. The terms used within UCR are defined in Appendix A, Definitions, Abbreviations and Acronyms, and References.~~

Requirements may be designated as "Required," "Conditional, or "Objective" requirements. The terms are defined in UCR, Appendix A Definitions, Abbreviations and Acronyms, and References. To illustrate the use of "Conditional," the statement "**[Conditional: R, LS~~]~~ ~~If~~] If** the product supports mobile users, the product shall support the Mobile IP Management MIBs as described in RFC 4295 (UCR 201~~0~~)" should be read to mean that the requirement to support the sections of the RFC 4295 would not be mandatory for all IPv6 routers and LAN switches, but is mandatory for products that are intended to support mobile users. Also, this requirement would take effect as part of UCR 2012.

The requirements defined in Section 5.3.2, Assured Services Requirements, are associated with the external interfaces of the UC products or network appliances (NAs). For defining each requirement, the terms "UC products" and "NAs" are shortened to "system." As shown in Figure 5.3.2-1, High-Level DISN Assured Services Network Model, the external interfaces for an NA are generally considered to be interfaces that connect to and interact with the ASLAN or the non-ASLAN. The primary interfaces associated with the IPv6 requirements are the signaling, AS-SIP, and bearer, SRTP interfaces.

~~LAN Switches can be either Layer 3 switches (with IP routing functions) or Layer 2 switches (without IP routing functions) within the ASLAN. In Section 5.3.5.3, Interim UC IPv6 Rules of Engagement, only Layer 3 LS must be IPv6 capable.~~
DoD IPv6 Standard Profile for IPv6 Capable Products, Version 5.0, defines the differences of various LAN switches as follows:

Layer-2 Switch: *A Switch that forwards based on Layer-2 only (MAC address) is a Layer-2 Switch. Note that unmanaged Layer-2 Switch can be described as a "pure" Layer 2 switch; it operates at Layer 2 only and is transparent at the IP layer. As such it has no IPv6-specific requirements and plays no active role as an IPv6 Capable product. A Layer-2 Switch may have some limited layer-3 control plane functions but is primarily a data plane device. A managed Layer-2 Switch product includes SNMP management or other user access via an IPv6 interface and it should be evaluated as a Simple Server.*

Layer-3 Switch: *A Switch that incorporates Layer-3 information (IP addresses) into forwarding decisions is a Layer-3 Switch. Forwarding may be manually configured, policy-based or based on routing protocols (BGP, RIP, OSPFv3 or IS-IS). Most Layer-3 Switches require a router gateway to connect the LAN/intranet to the Internet. The most capable Layer-3 Switches include a WAN interface and an exterior routing protocol such as BGP.*

Assured Services Switch: *A Switch that includes support for Quality of Service (QoS) features including the Differentiated Services Code Point (DSCP) queuing [RFC 2474] is an Assured Services Switch. DSCP queuing is an essential capability in the Unified Communications architecture to provide for Assured Services. Rather than being a separate Product Class, the requirements for Assured Services are specified as Conditional Requirements for compatibility with UCR 2010.*

For UCR 2010, this third category of switch is called LAN Access Switch which is required to support RFC 2460/5095, RFC 2464, and be able to queue packets based on DSCPs in accordance with RFC 2474. The complete set of RFCs for LAN Switches is listed in Table 5.3.5-5. (LS): Part 1 is LAN Access Switch, Part 2 is L3 Switch, and Part 3 is L3 Switch (Edge Router).

Finally, whenever a reference to a specific RFC appears in a UCR requirement, the specific language of the UCR requirement and its subtended requirements should be understood within the context of the RFC. The acronyms used for designating the appliances that a requirement pertains to are shown in Table 5.3.5-1, IPv6 Requirements for UCR 2010 Products. ~~and/or Function.~~

Table 5.3.5-1. IPv6 Requirements for UCR 2010 Products ~~and/or Function~~

DOD IPv6 PROFILE PRODUCT CLASS ~~UC PRODUCT OR FUNCTION~~	UCR 2010 PRODUCT NAME~~DOD IPv6 PROFILE CATEGORY~~	UCR 2010 IPv6 REQUIREMENTS [1, 2, 3]
Network Appliance or Simple Server (NA/SS)~~Multifunction Softswitch (MFSS)~~	Multifunction Softswitch (MFSS). ~~Network Appliance or Simple Server (NA/SS)~~	The MFSS/Call Control Agent (CCA) application in conjunction with the Voice and Video over IP (VVoIP) End Instrument (EI) and Media Gateway (MG)[4] must be IPv6-capable. Other applications within this APL product have a conditional requirement to be IPv6-capable if the IP packets remain internal to the product.
NA/SS~~Local Session Controller (LSC)~~	Local Session Controller (LSC)~~NA/SS~~	The LSC/CCA application in conjunction with the VVoIP EI and MG[4] must be IPv6-capable. Other applications in the APL product have a conditional requirement to be IPv6-capable.
NA/SS~~Video Telephony Unit (VTU)~~	Video Telephony Unit (VTU)~~NA/SS~~	If the VTU has an IP interface, the VTU must be IPv6-capable.
NA/SS~~Multipoint Control Unit (MCU)~~	Multipoint Control Unit (MCU)~~NA/SS~~	If the MCU has an IP interface, the MCU must be IPv6-capable.
NA/SS~~End Instrument (EI)~~	End Instrument (EI)~~NA/SS~~	The EI in conjunction with the CCA application must be IPv6-capable. This requirement is applicable for EIs manufactured after January 2009. Softphones and soft videophones have a conditional requirement for IPv6.

DOD IPv6 PROFILE PRODUCT CLASS ~~UC PRODUCT OR FUNCTION~~	UCR 2010 PRODUCT NAME~~DOD IPv6 PROFILE CATEGORY~~	UCR 2010 IPv6 REQUIREMENTS [1, 2, 3]
NA/SS	Standalone Product	If the UC Product, such as voice mail, call forwarding, call transfer, call waiting, operator assistance, and local directory services, is a standalone product then the DoD IPv6 Profile NA/SS requirements must apply, and the product must interoperate with vendor EIs that support IPv6
NA/SS~~Customer Premise Equipment (CPE)~~	Customer Premise Equipment (CPE)~~NA/SS~~	With exception of EIs, the CPE have a conditional requirement for IPv6 capability.
NA/SS~~Network Element (NE)~~	Network Element (NE)~~NA/SS~~	Conditional requirement for IPv6.
NA/SS~~Echo Canceller (EC)~~	Echo Canceller (EC)~~NA/SS~~	Conditional requirement for IPv6.
NA/SS~~Integrated Access Switch (IAS)~~	Integrated Access Switch (IAS)~~NA/SS~~	Conditional requirement for IPv6.
NA/SS~~Conference Bridge (external) (CB)~~	Conference Bridge (external) (CB)~~NA/SS~~	Conditional requirement for IPv6.
NA/SS~~H.323/H.320 Gateway (GW)~~	H.323 Gateway (GW) ~~NA/SS~~	H.323 Conditional requirement for IPv6. [5]
NA/SS	H.323 Gatekeeper (GK)	H.323 Conditional requirement for IPv6. [5]
NA/SS	Storage Devices	Conditional requirement for IPv6
NA/SS	Multifunction Mobile Devices	Conditional requirement for IPv6
Information Assurance Device~~de~~~~Edge Boundary Controller (EBC)~~	Edge Boundary Controller (EBC)~~Information Assurance Device~~	Must be IPv6-capable.
Information Assurance ~~Devide~~Device~~Intrusion Protection Systems (IPS) and Intrusion Detection Systems (IDS)~~	Intrusion Protection Systems (IPS) and Intrusion Detection Systems (IDS)~~Information Assurance Device~~	Must be capable of inspecting both IPv4 and IPv6 packets.

DOD IPv6 PROFILE PRODUCT CLASS ~~UC PRODUCT OR FUNCTION~~	UCR 2010 PRODUCT NAME~~DOD IPv6 PROFILE CATEGORY~~	UCR 2010 IPv6 REQUIREMENTS (1, 2, 3)
Information Assurance ~~Devide~~Device~~Firewalls (FW)~~	Firewalls (FW)~~Information Assurance Device~~	Must be IPv6-capable.
Information Assurance ~~Devide~~Device~~VPN Concentrator (VPN)~~	VPN Concentrator (VPN)~~Information Assurance Device~~	Must be IPv6-capable.
Assured Services Switch~~LAN Switch (LS)~~	LAN Switch (LS)~~Layer 3 Switch~~	Must be IPv6-capable.
Router~~Router (R)~~	Router (R) ~~Router~~	Must be IPv6-capable.
Various	Legacy systems of ~~:~~ ~~-~~Multifunction Switch (MFS)/Tandem Switch, ~~-~~End Office Switch (EOS)~~,~~, ~~-~~Small End Office (SMEO), ~~-~~Deployed Voice Exchange (DVX), ~~-~~Private Branch Exchange ~~1~~(PBX1), and PBX2. ~~Private Branch Exchange 2 (PBX2)~~	IPv6 ROE for legacy systems are spelled out in the Interim IPv6 ROE for UCR 2008 Change 1 at the UCCO web site http://www.disa.mil/ucco/apl_process.html

DOD IPv6 PROFILE PRODUCT CLASS ~~UC PRODUCT OR FUNCTION~~	UCR 2010 PRODUCT NAME~~DOD IPv6 PROFILE CATEGORY~~	UCR 2010 IPv6 REQUIREMENTS (1, 2, 3)

~~Notes:~~

~~1. The terms "Conditional requirement for IPv6" and "Other applications within the APL product have a conditional requirement to be IPv6-capable" effectively mean that the IPv6-capable features for the indicated UCR IPv6 application is optional and not required for listing on the UC APL.~~

~~2. While there is a requirement to manage IPv6 networks, the NM may be done using IPv4. Thus, NM is not included in this list.~~

~~3. Components within the UC products for which the IP packets remain internal to the SUT are not required to be IPv6-capable at this time, such as voice mail systems. In these cases, the resulting product can only be fielded within a B/P/C/S boundary. End instruments are required to be IPv6-capable regardless of placement within the SUT as indicated in this table. The UC APL certification shall reflect conditions under which the product was certified. The product is to be fielded within B/P/C/S boundaries. For the cases where components are within the UC products and the IP packets remain internal to the System Under Test (SUT) without using the DISN WAN, (i.e. the external interface for the SUT for signaling traffic and bearer traffic are TDM/serial and IP is only used for external network management) the internal interfaces for the SUT are not required to be IPv6 and the product would not have to support IPv6 at this time. These components provide services as described in Section 5.3.2.24 *Requirements for Supporting AS-SIP-Based Ethernet Interfaces for Voicemail, Unified Messaging Systems, and Automated Receiving Devices.* The resulting UC product can only be fielded within a B/P/C/S boundary. This guidance would apply for both generic AS-SIP End Instruments (EIs) and proprietary protocol EIs. The EIs are required to be IPv6-capable regardless of placement within the SUT as indicated in this table. The UC APL listing shall reflect conditions under which the product was certified.~~

~~4. The MG is only required to be IPv6-capable if it has an external IP interface to the SUT. In these cases, the resulting product can only be fielded within a B/P/C/S boundary. The UC APL certification shall reflect conditions under which the product was certified.~~

~~5. This requirement and H.323 sunset will be revisited for UCR 2012.~~

Notes: 1The terms "Conditional requirement for IPv6" and "Other applications within the APL product have a conditional requirement to be IPv6-capable" effectively mean that the IPv6-capable features for the indicated UCR IPv6 application is optional and not required for listing on the UC APL.

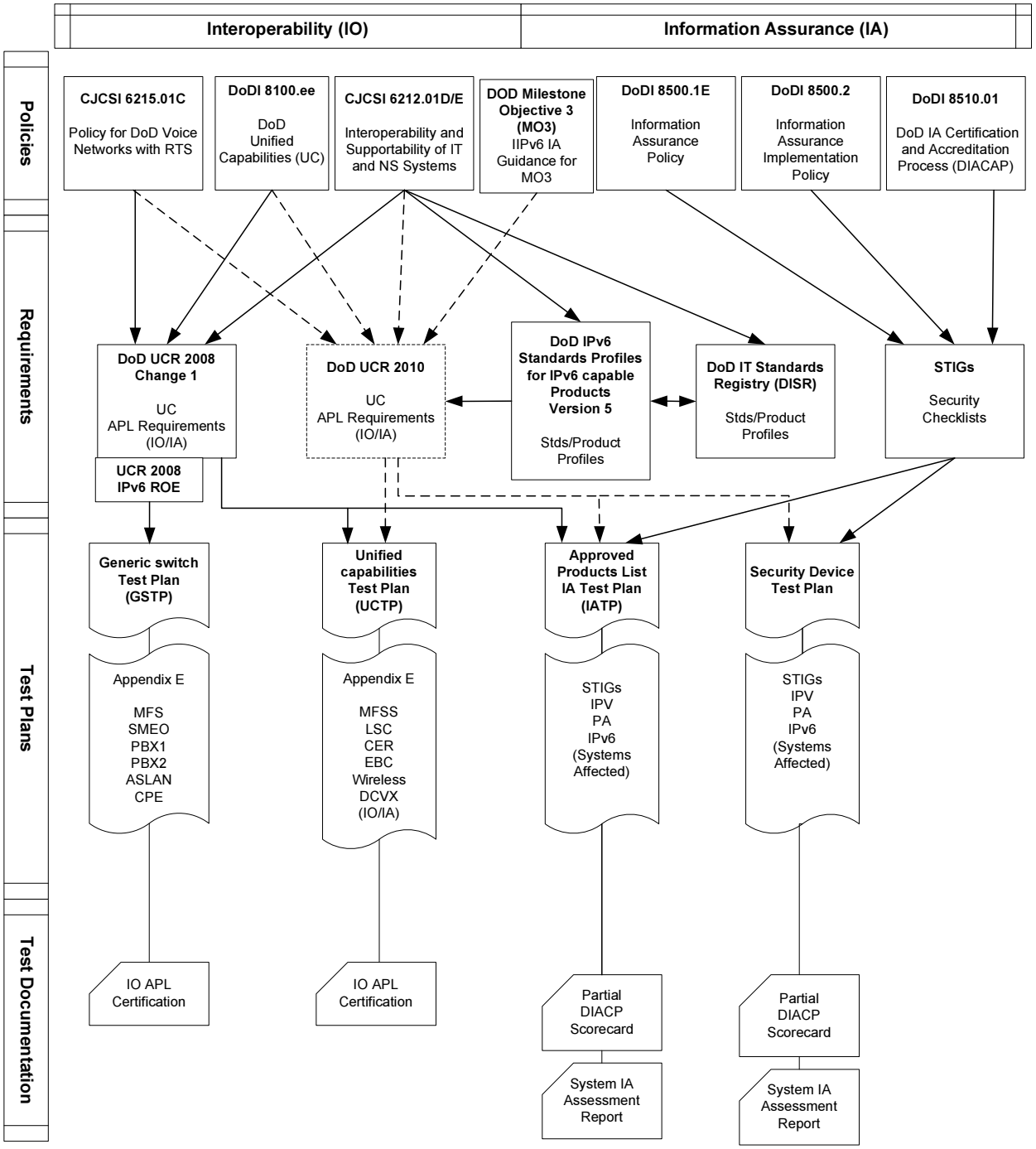
2. While there is a requirement to manage IPv6 networks, the NM may be done using IPv4. Thus, NM is not included in this list.

3. For the cases where components are within the UC products and the IP packets remain internal to the System Under Test (SUT) without using the DISN WAN, (i.e. the external interface for the SUT for signaling traffic and bearer traffic are TDM/serial and IP is only used for external network management) the internal interfaces for the SUT are not required to be IPv6 and the product would not have to support IPv6 at this time. These components provide services as described in Section 5.3.2.24 *Requirements for Supporting AS-SIP-Based Ethernet Interfaces for Voicemail, Unified Messaging Systems, and Automated Receiving Devices.* The resulting UC product can only be fielded within a B/P/C/S boundary. This guidance would apply for both generic AS-SIP End Instruments (EIs) and proprietary protocol EIs. The EIs are required to be IPv6-capable regardless of placement within the SUT as indicated in this table. The UC APL listing shall reflect conditions under which the product was certified.

4. The MG is only required to be IPv6-capable if it has an external IP interface to the SUT. In these cases, the resulting product can only be fielded within a B/P/C/S boundary. The UC APL certification shall reflect conditions under which the product was certified.

5. This requirement and H.323 sunset will be revisited for UCR 2012.

Below is a Document Tree showing the relationship among Policy, Requirements, Test Plans and Test Documents (for Interoperability and Information Assurance) for Listing on the UC APL.



5.3.5.3 ~~Interim~~ UCR 2010 IPv6 Rules of Engagement

The purpose of this section is to provide ~~interim~~ policy/~~ and~~ guidance/Rules of Engagement (RoE~~O~~E) to be used by the Government and industry to achieve UC APL status for IPv6-capable products. This set of IPv6 RoE~~O~~E applies to all industry vendors seeking to place products on the DoD UC APL. The UCCO and DISA JITC shall enforce this guidance in test and certification of vendor products that have IP capabilities. This guidance is effective immediately and supersedes any previous RoE~~O~~E Versions that have been issued.

5.3.5.3.1 Definitions

These definitions are derived from DoD Deputy CIO Memorandum "DoD IPv6 Definitions."

1. IPv6 Capable Products. Products (whether developed by commercial vendor or the government) that can create or receive, process, and send or forward (as appropriate) IPv6 packets in mixed IPv4/IPv6 environments. IPv6 capable products shall be able to interoperate with other IPv6 capable products on networks supporting only IPv4, only IPv6, or both IPv4 and IPv6, and shall also:

   (1) Conform to the requirements of the IPv6 profile in UCR 2010.

   (2) Possess a migration path and/or letter of commitment to upgrade from the developer (signed by company Vice President or equivalent) as the IPv6 standard evolves.

   (3) Ensure product developer IPv6 technical support is available.

   (4) Conform to National Security Agency (NSA) and/or Unified Cross Domain Management Office requirements for Information Assurance products.

2. System Under Test (SUT). The inclusive components required to test a UC product for APL certification. ~~Examples of a SUT include VoIP system components (e.g., LSC and gateway), LAN components (e.g., routers and Ethernet switches), and EIs.~~ Examples of a SUT include Voice over Internet Protocol (VoIP) system components (e.g., Local Session Controller (LSC) and gateway), Local Area Network (LAN) components (e.g., routers and Ethernet switches), and end instruments.

3. IPv6-Capable Networks. Networks that can receive, process, and forward IPv6 packets from/to devices within the same network and from/to other networks and systems, where

those networks and systems may be operating with only IPv4, only IPv6, or both IPv4 and IPv6. An IPv6-capable network shall be ready to have IPv6 enabled for operational use, when mission need or business case dictates. Specifically, an IPv6-capable network must:

a. Use IPv6-capable products.

b. Accommodate IPv6 in network infrastructures, services, and management tools and applications.

c. Conform to DoD and NSA-developed IPv6 network security implementation guidance.

d. Manage, administer, and resolve IPv6 addresses in compliance with the DoD IPv6 Address Plan when enabled.

4. IPv6-Enabled Network. An IP network that is supporting operational IPv6 traffic through the network, E2E.

5.3.5.3.2 IPv6 Rules of Engagement

1. IPv6 Requirements. Detailed IPv6 requirements for UC products and/or functions are provided in this section of the UCR. Table 5.3.5-1, IPv6 Requirements for Products and/or Function, provides a high-level listing of UC products or functions, DoD IPv6 Profile categories, and UCR IPv6 requirements to be considered IPv6-capable.

2. New IPv6 Requirements.

(1) According to ~~UCR 2008 Change 1~~ Section 4.6.3.1 Standard Process for Gaining APL Status: When a requirement addition, change, or deletion has been approved on the date the UCR is signed, one of five dispositions will occur as follows:

(a) The vendors will have 18 months to develop the requirement if it is new and not previously available. Vendors may provide it earlier.

Note: The 18-month period for development would apply to a new feature or a product not previously required, and the vendors did not have long-range knowledge of the requirement. New features or products are included in Table 4.6.3-2, New Features and Products in UCR 2010 for which 18-Month Rule Applies.

Note: With respect to the 18-month period, a vendor may request to NII/DoD-CIO a waiver for IPv6 requirements. Such requests should include a commitment to provide a migration path and corporate commitment to upgrade the product to be IPv6 compliant. Failure

to meet this commitment will remove the products from the APL, at the option of the NII/DoD-CIO.

(b) If the requirement has been lessened, vendor compliance is immediate.

(c) If warning of the requirements has been given before approval, the requirement compliance may be immediate.

(d) If the requirement addresses a Critical or Major IA risk, compliance is immediate .

(e) If the requirement is necessary for multivendor interoperability, compliance is immediate.

~~2~~3. UC APL Listing.

a. The DoD no longer supports standalone IPv6 product certification testing. For products identified in the UCR, IPv6 requirements will be validated in conjunction with the larger Interoperability certification and Information Assurance testing that is conducted on the product for listing on the UC APL.

b. Products that have been placed on the DoD UC APL as a result of vendor commitments, via an LOC, to be IPv6 capable (or other IPv6-related commitments) will be removed from the APL, and may be subject to other actions, if the vendor does not deliver on the commitment within 12 months of the LOC.

4. UC Distributed Test Concept

(1) According to DoDI 8000.ee DoD Unified Capabilities (UC), the following guidance relates to the UC Distributed Test Concept:

(a) DISA shall employ a distributed test capability that includes test and certification of voice, video, and data products to accommodate the expanded scope of the UCR, and to keep pace with emerging technology and the large demand from the OSD and DoD Components for interoperable and secure products.

(b) These demands and technology challenges require the Department of Defense to incorporate OSD and DoD Component test labs in the test and certification processes.

(c) The precepts of the distributed test program are to "test once for many," create a single DoD UC APL for use by the OSD and DoD Components in acquisitions and procurements, and more effectively integrate industry into the test and certification process.

5.3.5.4 Product Requirements

1. **[Required: NA/SS, R, EBC] [Conditional: EI]** The product shall support dual IPv4 and IPv6 stacks as described in RFC 4213.

   [Conditional: LS] If the LS also supports a routing function, the product shall support RFC 4213.

   NOTE: The tunnel requirements are only associated with appliances that provide IP routing functions (e.g., routers). The primary intent of these requirements is to (1) require dual stacks on all UC appliances and (2) allow dual stacks and tunneling on routers.

   1.1 **[Required: EI, NA/SS, R, LS, EBC]** Dual stack end points or Call Control Agents shall be configured to choose IPv4 over IPv6.

   NOTE: Most commercial vendors can configure their equipment to choose IPv4 or IPv6. JITC testing preference, for IPv6 features, is to test the equipment configured for IPv6 to insure that it can dynamically negotiate with IPv4 only end points.

   1.2 **[Required: EI, NA/SS, R, LS, EBC]** All nodes that are "IPv6-capable" shall be carefully configured and verified that the IPv6 stack is disabled until it is deliberately enabled as part of a risk management strategy. This includes the stateless auto configuration of link-local addresses.

   [Conditional: EI CY 2008-2012] The EIs are allowed to use alternative mechanisms (e.g., translation and tunneling) between CY 2008 and CY 2012 as long as performance, Interoperability, and Information Assurance requirements are met.

   NOTE: Translation based on RFC 2766, Network Address Translation – Protocol Translation (NAT-PT) is no longer supported in the IETF community and has been rendered *Historic* by the publication of RFC 4966 primarily for security concerns.

   1.3 **[Conditional: R, LS]** If the product supports routing functions, the product shall support the manual tunnel requirements as described in RFC 4213.

   1.4 **[Required: EI, NA/SS, R, LS, EBC]** Products which provide a function(s) in IPv4 will have to provide the same function(s) in a seamless manner when the product is

submitted for UC APL certification, or provide for a suitable substitute using IPv6 technologies. (For example, if a product from a vendor provides for IPSec in an EI using the Skinny Call Control Protocol (SCCP, or short Skinny) protocol in IPv4, the EI must provide for IPSec in IPv6 when using AS-SIP protocol when submitted for UC APL certification.)

2. **[Required: EI, NA/SS, R, EBC]** The product shall support the IPv6 format as described in RFC 2460 and updated by RFC 5095. **[Conditional: LS]** If the LS also supports a routing function, the product shall support RFC 2460 and updated by RFC 5095.

3. **[Required: EI, NA/SS, R, LS, EBC]** The product shall support the transmission of IPv6 packets over Ethernet networks using the frame format defined in RFC 2464.

   NOTE: This requirement does not mandate that the remaining sections of RFC 2464 have to be implemented.

5.3.5.4.1 Maximum Transmission Unit

4. **[Required: EI (Softphone Only), R, EBC]** The product shall support Path Maximum Transmission Unit (MTU) Discovery (RFC 1981). **[Conditional: LS]** If the LS supports a routing function, the product shall support RFC 1981.

5. **[Required: EI, NA/SS, R, LS, EBC]** The product shall support a minimum MTU of 1280 bytes (RFC 2460 and updated by RFC 5095).

   NOTE: Guidance on MTU requirements and settings can be found in Section 5.3.3.10.1.2, Layer 2 Data Link Layer.

6. **[Conditional: EI, NA/SS, R, LS, EBC]** If Path MTU Discovery is used and a "Packet Too Big" message is received requesting a next-hop MTU that is less than the IPv6 minimum link MTU, the product shall ignore the request for the smaller MTU and shall include a fragment header in the packet.

   NOTE: This is to mitigate an attack where the path MTU is adequate, but the "Packet Too Big" messages are used to make the packet so small it is inefficient.

5.3.5.4.2 Flow Label

7. **[Required: EI, NA/SS, EBC]** The product shall not use the Flow Label field as described in RFC 2460.

7.1 **[Required: EI, NA/SS, EBC]** The product shall be capable of setting the Flow Label field to zero when originating a packet.

7.2 **[Required: NA/SS, EBC]** The product shall not modify the Flow Label field when forwarding packets.

7.3 **[Required: EI, NA/SS, EBC]** The product shall be capable of ignoring the Flow Label field when receiving packets.

5.3.5.4.3 Address

8. **[Required: EI, NA/SS, R, LS, EBC]** The product shall support the IPv6 Addressing Architecture as described in RFC 4291.

NOTE: According to "DoD IPv6 Standard Profiles For IPv6-capable Products-Supplemental Guidance" version 3.0, the use of "IPv4-mapped" addresses "on-the-wire" is discouraged due to security risks raised by inherent ambiguities.

NOTE: As noted in NIST SP500-267 25 "A Profile for IPv6 in the U.S. Government – Version 1.0": "The use of the old Site-Local address type [RFC3879] is deprecated. The Unique Local IPv6 Unicast Addresses (ULA) [RFC 4193] mechanism has been designed to fulfill a similar requirement. While Private Addresses are widely used in IPv4 networks, the generalized use and support of ULAs in IPv6 is not as mature nor is their architectural desirability as well understood." For these reasons, the UC products are not required to support ULA at this time.

8.1 An end site is defined as an end-user (subscriber) edge network domain that requires multiple subnets/64 as defined in Section 5.1, End-Site Definition of DoD IPv6 Address Plan. Therefore, vendors will not be required to support anything greater than /64, such as /116 or /126 subnet.

9. **[Required: EI, NA/SS, R, LS, EBC]** The product shall support the IPv6 Scoped Address Architecture as described in RFC 4007.

9.1 **[Conditional: EI, NA/ SS, R, LS, EBC]** If a scoped address (RFC 4007) is used, the product shall use a scope index value of zero when the default zone is intended.

9.2 Reserved.

5.3.5.4.4 DHCP

10. **[Required: EI~~IE]~~] [Conditional: NA/SS, R]** If DHCP is supported within an IPv6 environment, it shall be implemented in accordance with the DHCP for IPv6 (DHCPv6) as described in RFC 3315.

[Conditional: LS] If the LS also supports a routing function, the product shall support RFC 3315.

NOTE 1 : Section 5.4.5.4.2 describes the registration of the appliance to the network and its receipt of an E.164 telephone number if it is an EI or an Assured Services Session Initiation Protocol (AS-SIP) End Instrument (AEI). During the initial installation of an appliance either it will be configured with a static IP address (i.e., LSC, SS, MG, MFSS, AEI, and EI) or will receive its (EI or AEI) IP address from a DHCP server. The first step is for the EI or AEI to authenticate itself to the LAN switch to which it is physically connected, If DHCP is used, when the EI or AEI authenticates itself to the DHCP server to get its IP address it will also obtain the registration information necessary to locate the LSC. If an EI uses static IP addresses, it will be preconfigured by the system administrator with the location information of the LSC.

NOTE 2: Section 5.4, Information Assurance, requires that the voice or video DHCP servers are not to be located on the same physical appliance as the voice or video LAN switches and routers in accordance with the STIGs. Also, the VoIP STIG requires (in VoIP 0082) separate DHCP servers for (1) the telephone system in the phone VLAN(s) and (2) the data devices (PCs) in the data VLAN(s).

NOTE 2: There is no requirement that separate DHCP servers be used for IPv4 and for IPv6.

10.1 **[Conditional: EI, NA/SS]** If the product is a DHCPv6 client, the product shall discard any messages that contain options that are not allowed to appear in the received message type (e.g., an Identity Association option in an Information-Request message).

10.2 **[Required: EI]** The product shall support DHCPv6 as described in RFC 3315. NOTE: The following subtended requirements are predicated upon an implementation of DHCPv6 for the EI. It is not expected that other UC appliances will use DHCPv6.

10.2.1 **[Required: EI] [Conditional: NA/SS]** If the product is a DHCPv6 client, and the first retransmission timeout has elapsed since the client sent the Solicit message and the client has received an Advertise message(s), but the Advertise message(s) does not have a preference value of 255, the client shall

continue with a client-initiated message exchange by sending a Request message.

10.2.2 **[Required: EI – Conditional: NA/SS]** If the product is a DHCPv6 client and the DHCPv6 solicitation message exchange fails, it shall restart the reconfiguration process after receiving user input, system restart, attachment to a new link, a system configurable timer, or a user defined external event occurs.

NOTE: The intent is to ensure that the DHCP client continues to restart the configuration process periodically until it succeeds.

10.2.3 **[Required: EI – Conditional: NA/SS]** If the product is a DHCPv6 client and it sends an Information-Request message, it shall include a Client Identifier option to allow it to be authenticated to the DHCPv6 server.

10.2.4 **[Required: EI – Conditional: NA/SS]** If the product is a DHCPv6 client, it shall perform duplicate address detection upon receipt of an address from the DHCPv6 server before transmitting packets using that address for itself.

10.2.5 **[Required: EI – Conditional: NA/SS]** **[Alarm]** If the product is a DHCPv6 client, it shall log all reconfigure events.

NOTE: Some systems may not be able to log all this information (e.g., the system may not have access to this information).

10.3 **[Conditional: EI, NA/SS, R, LS]** **[Alarm]** If the product supports DHCPv6 and uses authentication, it shall discard unauthenticated DHCPv6 messages from UC products and log the event.

NOTE 1: This requirement assumes authentication is used as described in RFC 3118 (and extended in RFC 3315) but does not require authentication.

NOTE 2: Some systems may not be able to log all this information (e.g., the system may not have access to this information).

5.3.5.4.5 Neighbor Discovery

11. **[Required: EI, NA/SS, R, EBC]** The product shall support Neighbor Discovery for IPv6 as described in ~~RFC 2461 and~~ RFC 4861 ~~(UCR 2010)~~.

[Conditional: LS] If the LS also supports a routing function, the product shall support RFC ~~2461 and RFC~~ 4861 ~~(UCR 2010)~~.

NOTE: RFC 4861 replaced the now obsolete RFC 2461.

~~NOTE: For ICMPv6 Neighbor Discovery functions specified by RFC 2461 (Router Advertisement/Solicitation, Neighbor Advertisement/Solicitation, and Redirect) the preferred DSCP for ICMPv6 neighbor discovery related packets is DSCP 0, which is defined in Section 5.3.3, Network Infrastructure End-to-End Performance Requirements for Granular Service Class of Best Effort.~~

11.1 **[Required: NA/SS, R, LS, EBC]** The product shall not set the override flag bit in the Neighbor Advertisement message for solicited advertisements for anycast addresses or solicited proxy advertisements.

11.2 Reserved.

11.3 **[Required: EI, NA/SS, R, LS, EBC]** When a valid "Neighbor Advertisement" message is received by the product and the product neighbor cache does not contain the target's entry, the advertisement shall be silently discarded.

11.4 **[Required: EI, NA/SS, R, LS, EBC]** When a valid "Neighbor Advertisement" message is received by the product and the product neighbor cache entry is in the INCOMPLETE state when the advertisement is received and the link layer has addresses and no target link-layer option is included, the product shall silently discard the received advertisement.

11.5 **[Required: EI, NA/SS, R, LS, EBC]** When address resolution fails on a neighboring address, the entry shall be deleted from the product's neighbor cache.

5.3.5.4.5.1 Redirect Messages

11.6 **[Required: EI, NA/SS, EBC]** The product shall support the ability to configure the product to ignore Redirect messages.

11.7 **[Required: EI, NA/SS, EBC]** The product shall only accept Redirect messages from the same router as is currently being used for that destination.

NOTE: The intent of this requirement is that if a node is sending its packets destined for location A to router X, that it can only accept a Redirect message from router X for packets destined for location A to be sent to router Z.

11.7.1 **[Conditional: EI, NA/SS~~, EBC~~]** If "Redirect" messages are allowed, the product shall update its destination cache in accordance with the validated Redirect message.

11.7.2 **[Conditional: EI, NA/SS~~, EBC~~]** If the valid "Redirect" message is allowed and no entry exists in the destination cache, the product shall create an entry.

11.7.3 [Conditional: EI, NA/SS] If redirects are supported, the device shall support the ability to disable this functionality.

NOTE: The default setting is "disabled" so that the redirect functions must explicitly be enabled."

5.3.5.4.5.2 Router Advertisements

11.8 **[Required: R] [Conditional: LS]** **[Alarm]** If the product supports routing functions, the product shall inspect valid router advertisements sent by other routers and verify that the routers are advertising consistent information on a link and shall log any inconsistent router advertisements.

NOTE: Some products may not be able to log all this information (e.g., the product may not have access to this information).

11.8.1 **[Required: EI, NA/SS, EBC]** The product shall prefer routers that are reachable over routers whose reachability is suspect or unknown.

11.8.2 Reserved.

11.9 **[Required: R] [Conditional: LS]** If the product supports routing functions, the product shall include the MTU value in the router advertisement message for all links in accordance with RFC ~~2461 and RFC~~ 4861 ~~(UCR 2010)~~.

5.3.5.4.6 Stateless Address Autoconfiguration and Manual Address Assignment

12. **[Conditional: EI, NA/SS, R, LS, EBC]** If the product supports stateless IP address autoconfiguration including those provided for the commercial market, the product shall support IPv6 Stateless Address Autoconfiguration (SLAAC) for interfaces supporting UC functions in accordance with ~~RFC 2462 and~~ RFC 4862 ~~(UCR 2010)~~.

NOTE 1: RFC 4862 replaced the now obsolete RFC 2462. The scope of RFC 2462, Section 5.5, is Creation of Global and Site-Local Addresses. The scope of RFC 4862, Section 5.5, is Creation of Global Addresses.

NOTE 2: "DoD IPv6 Standard Profiles for IPv6-capable Products-Supplemental Guidance" defines Host as a PC or other end-user computer or workstation running a general-purpose operating system.

NOTE 3: The UC EI platform (on which the softphone is located) may be certified to the DoD IPv6 Profile and required to support autonomous configuration, either SLAAC or DHCPv6 client.

~~NOTE: The scope of RFC 2462, Section 5.5, is Creation of Global and Site-Local Addresses. The scope of RFC 4862, Section 5.5, is Creation of Global Addresses.~~

~~12.1 **[Conditional: SS, NA, EBC, EI]** If the product supports IPv6 SLAAC, the product shall have a configurable parameter that allows the function to be enabled and disabled.~~

~~NOTE: The objective of this requirement is to prevent a product from using stateless auto configuration.~~

~~NOTE: An alternative to the configurable parameter, the IPv6 SLAAC functions may be removed from the operating system of the IPv6 node.~~

~~12.1.1 **[Conditional: EI, NA/ SS, R, LS, EBC]** If the product supports IPv6 SLAAC, the product shall have a configurable parameter that allows the "managed address configuration" flag and the "other stateful configuration" flag to always be set and not perform stateless autoconfiguration.~~

~~NOTE: The objective of this requirement is to prevent a product from using stateless auto configuration.~~

12.1 **[Conditional: EI, NA/ SS, R, LS, EBC]** If the product supports IPv6 SLAAC, the product shall have a configurable parameter that allows the function to be enabled and disabled. Specifically, the product shall have a configurable parameter that allows the "managed address configuration" flag and the "other stateful configuration" flag to always be set and not perform stateless autoconfiguration.

12.1.1 **[Conditional: EI (except softphones), NA/ SS, R, LS, EBC]** If the product supports IPv6 SLAAC, the product shall have the configurable parameter set not to perform stateless autoconfiguration.

NOTE: The objective of this requirement is to prevent a product from using stateless auto configuration. Basically, stateless address autoconfiguration is focused solely on softphones since they reside on PCs. The concern is that when an appliance uses

SLAAC the appliance can dynamically change its IP address (during a power recycle or other reasons). For EIs (exception Softphones) UCR 2010 requires the use static or DHCP. For the rest of the appliances, UCR 2010 requires static IP addresses. The table below summarizes this policy guidance.

UC Product	**Manual IPv6 Configuration?**	**IPv6 Stateful Configuration via DHCPv6?**	**IPv6 StateLess Address AutoConfiguration (SLAAC)?**
Softphones	Yes, Requirement 12.3	Yes, Requirement 10	Yes, Requirement 12.4
EI (except softphones)	Yes, Requirement 12.3	Yes, Requirement 10	No, Requirement 12.1.1
NA/SS	Yes, Requirement 12.3	No for LSC, SS, MG, MFSS, Requirement 10, Note 1. Yes for all others, Requirement 10 Conditional on RFC 3315	No, Requirement 12.1.1
R	Yes, Requirement 12.3	Yes, Requirement 10, Conditional on RFC 3315	No, Requirement 12.1.1
LS	Yes, Requirement 12.3	No, Requirement 10	No, Requirement 12.1.1
EBC	Yes, Requirement 12.3	No, Requirement 10	No, Requirement 12.1.1

Where" No"could be (1) not installed, (2) removed from Operating System, or (3) disabled by parameter.

~~12.2 [**Conditional: EI, NS/NA, R, LS, EBC]** If the product supports stateless IP address autoconfiguration including those provided for the commercial market, the DAD shall be disabled in accordance with RFC 2462 and RFC 4862 (UCR 2010).~~ 12.2 [**Required: EI, NS/NA, R, LS, EBC]** While nodes are not required to autoconfigure their addresses using SLAAC, all IPv6 Nodes shall support link-local address configuration and Duplicate Address Detection (DAD) as specified in RFC 4862 and, in accordance with RFC 4862, the DAD shall not be disabled.

12.2.1 [**Required: EI, NS/NA, R, LS, EBC]** A node MUST allow for autoconfiguration-related variable to be configured by system management for each multicast-capable interface to include DupAddrDetectTransmits where a value of zero indicates that Duplicate Address Detection is not performed on tentative addresses as specified in RFC 4862.

NOTE: NETWORK INFRASTRUCTURE Security Technical Implementation Guide (STIG) states that: "The use of Duplicate Address Detection opens up the possibility of denial of service attacks. Any node can respond to Neighbor Solicitations for a tentative address, causing the other node to reject the address as

a duplicate. This attack is similar to other attacks involving the spoofing of Neighbor Discovery messages."
Further, RFC 4862 states: "By default, all addresses should be tested for uniqueness prior to their assignment to an interface for safety. The test should individually be performed on all addresses obtained manually, via stateless address autoconfiguration, or via DHCPv6. To accommodate sites that believe the overhead of performing Duplicate Address Detection outweighs its benefits, the use of Duplicate Address Detection can be disabled through the administrative setting of a per-interface configuration flag."

12.3 **[Required: EI, NA/SS, R, LS, EBC]** The product shall support manual assignment of IPv6 addresses.

12.4 **[Required: EI]** The product shall support stateful autoconfiguration (i.e., ManagedFlag=TRUE).

NOTE: This requirement is associated with the earlier Requirement 10.2 for the EI to support DHCPv6.

12.4.1 **[Required: R] [Conditional: LS]** If the product provides routing functions, the product shall default to using the "managed address configuration" flag and the "other stateful flag" set to TRUE in their router advertisements when stateful autoconfiguration is implemented.

12.5 **[Conditional: EI]** If the product supports a subtended appliance behind it, the product shall ensure that the IP address assignment process of the subtended appliance is transparent to the UC components of the product and does not cause the product to attempt to change its IP address.

NOTE: An example is a PC that is connected to the LAN through the hub or switch interface on a phone. The address assignment process of the PC should be transparent to the EI and should not cause the phone to attempt to change its IP address.

12.6. **[Conditional: EI (Softphones only)]** If the product supports SLAAC and security constraints prohibit the use of hardware identifiers as part of interface addresses generated using SLAAC, IPSec-capable products shall support privacy extensions for stateless address autoconfiguration as defined in RFC ~~3041 and RFC~~ 4941 ~~(UCR 2010)~~.

NOTE: RFC 4941 replaced the now obsolete RFC 3041.

13. Reserved.

5.3.5.4.7 Internet Control Message Protocol

14 **[Required: EI, NA/SS, R, LS, EBC]** The product shall support the ICMPv6 as described in RFC 4443. ~~**[Conditional: LS]** If the LS supports a routing function, the product shall support RFC 4443.~~

NOTE: Section 5.3.1.3.5 Protocols states that the Core, Distribution, and Access products shall meet the IPv4 protocol requirements for RFC 1256 ICMP (PING). Thus, support for RFC 4443 for Core, Distribution, and Access products should be ICMP (PING).

14.1 **[Required: NA/SS, R, EBC]** The product shall have a configurable rate limiting parameter for rate limiting the forwarding of ICMP messages.

[Conditional: LS] If the LS supports a routing function, subtended requirement 14.1 applies.

14.2 **[Required: NA/SS, R, LS, EBC]** The product shall support the capability to enable or disable the ability of the product to generate a Destination Unreachable message in response to a packet that cannot be delivered to its destination for reasons other than congestion.

Note: In lieu of RFC4443 paragraph 3.1 requirement to prohibit routers from forwarding Destination Unreachable message with a code 3 (Address unreachable) on point-to-point link back onto the arrival link, vendors may alternatively use a prefix length of 127 on Inter-Router Links to address ping pong issues on non-Ethernet interfaces (the ping pong issue is not present on Ethernet interfaces) [Ref: Draft RFC "Using 127-bit IPv6 Prefixes on Inter-Router Links draft-kohno-ipv6-prefixlen-p2p-01.txt"]

~~**[Conditional: LS]** If the LS supports a routing function, subtended Requirement 14.2 applies.~~

14.3 **[Required: EI, NA/SS, R, LS, EBC]** The product shall support the enabling or disabling of the ability to send an Echo Reply message in response to an Echo Request message sent to an IPv6 multicast or anycast address.

~~**[Conditional: LS]** If the LS supports a routing function, subtended Requirement 14.3 applies.~~

NOTE: The number of responses may be traffic conditioned to limit the effect of a denial of service attack.

14.4 **[Required: EI, NA/SS, R, EBC]** The product shall validate ICMPv6 messages, using the information contained in the payload, before acting on them.

Note: The actual validation checks are specific to the upper layers and are out of the scope of this UCR. Protecting the upper layer with IPSec mitigates these attacks.

[Conditional: LS] If the LS supports a routing function, subtended Requirement 14.4 applies.

5.3.5.4.8 Routing Functions

15. **[Required: R] [Conditional: LS]** If the product supports routing functions, the product shall support the OSPF for IPv6 as described in RFC ~~2740~~5340.

NOTE: RFC 5340 replaced the now obsolete RFC 2740.

15.1 **[Required: R] [Conditional: LS]** If the product supports routing functions, the product shall support securing OSPF with IPSec as described for other IPSec instances in Section 5.4, Information Assurance.

15.2. **[Required: R] [Conditional: LS]** If the product supports routing functions, the product shall support router-to-router integrity using the IP Authentication Header with HMAC-SHA1-96 within ESP and AH as described in RFC 2404.

NOTE: NIST Special Publication 500-267, "A Profile for IPv6 in the U.S. Government," forwards the following guidance: Although HMAC-SHA-1 [RFC 2404] is still considered secure, the IETF is encouraging the standardization of HMAC-SHA-256 to ensure an orderly transition to a more secure MAC.

15.3 **[Required: R] [Conditional: LS]** If the product supports interior routing functions of OSPFv3, the product shall support RFC 4552.

NOTE: RFC 4552 relies on manual key exchange (pre-configuration) and may not be appropriate in a dynamic tactical environment. Router acquisitions for tactical deployment are exempt from this requirement.

15.4 **[Required: R] [Conditional: LS]** If the product supports interior routing functions of and the address families in OSPFv3, the product shall support RFC 5838 (UCR 2012).

NOTE: RFC 5838 "Support of Address Families in OSPFv3" discussing the approach to handling multiple Address Families in OSPFv3 using multiple instances. This will be useful in the dual-stack environment for supporting both IPv4 and IPv6 routing domains.

15a. **[Required: R] [Conditional: LS]** If the product supports the Intermediate System to Intermediate System (IS-IS) routing protocol used in DoD backbone networks, the product shall support the IS-IS for IPv6 as described in RFC 5308 ~~(UCR 2010)~~.

15a.1 **[Required: R] [Conditional: LS]** If the product supports IS-IS routing architecture (for IPv6-only or dual-stack operation) the product shall support RFC 5304 ~~(UCR 2010)~~ and RFC 5310 ~~(UCR 2010)~~.

NOTE: IS-IS implementers should monitor further specification of ancillary features in the IETF ISIS Working Group, including http://tools.ietf.org/html/draft-ietf-isis-ipv6-te-06 on traffic engineering.

16. **[Conditional: R, LS]** If the product acts as a CE Router, the product shall support the use of BGP as described in RFC 1772 and RFC 4271.

16.1. **[Conditional: R, LS]** If the product acts as a CE Router, the product shall support the use of BGP4 multiprotocol extensions for IPv6 inter-domain routing (RFC 2545).

NOTE: The requirement to support BGP4 is in Section 5.3.3, Wide Area Network General System Requirements.

17. [**Conditional: R, LS]** If the product acts as a CE Router, the product shall support multiprotocol extensions for BGP4 in R~~RFC 2858 and R~~FC 4760 ~~(UCR 2010)~~.

NOTE1: RFC 4760 replaced the now obsolete RFC 2858.

NOTE 2: The requirement to support BGP4 is in Section 5.3.3, Wide Area Network General System Requirements.

18. [**Conditional: R]** If the product acts as a CE Router, the product shall support the Generic Routing Encapsulation (GRE) as described in RFC 2784.

19. [**Conditional: R]** If the product acts as a CE Router, the product shall support the Generic Packet Tunneling in IPv6 Specification as described in RFC 2473.

    NOTE: Tunneling is provided for data applications and is not needed as part of the VVoIP architecture.

20. **[Required: EI (Softphone Only), R] [Conditional: LS]** If the product supports routing functions, the product shall support the Multicast Listener Discovery (MLD) process as described in RFC 2710 and extended in RFC 3810.

    NOTE: The CY 2008 VVoIP design does not use multicast, but routers supporting VVoIP also support data applications that may use multicast. A softphone will have non-routing functions that require MLDv2.

    20.1 **[Required: EI (Softphone Only), R] [Conditional: LS]** If the product supports MLD process as described in RFC 2710 and extended in RFC 3810, the product shall support RFC 2711.

21. **[Required: EI, NA/SS, EBC]** The product shall support MLD as described in RFC 2710.

    NOTE: This requirement was added to ensure that Neighbor Discovery multicast requirements are met. Routers are not included in this requirement since they have to meet RFC 2710 in the preceding requirement.

5.3.5.4.9 IP Security

22. **[Required: EI (Softphone Only), R] [Conditional: EI, NA/SS, LS, EBC]** If the product uses IPSec, the product shall support the Security Architecture for the IP ~~RFC 2401 and~~ RFC 4301 ~~(UCR 2010)~~.

    NOTE 1: RFC 4301 replaced the now obsolete RFC 2401.

    NOTE 2: ~~In CY 2009,~~ RFC 2401 (and its related RFCs) is the Threshold requirement as described in Section 5.4, Information Assurance. In addition, the interfaces required to use IPSec are defined in Section 5.4, Information Assurance.

    22.1 **[Required: EI (Softphone Only), R] [Conditional: EI, NA/SS, LS, EBC]** If RFC 4301 is supported, the product shall support binding of a security association (SA) with a particular context.

22.2 **[Required: EI (Softphone Only), R] [Conditional: EI, NA/SS, LS, EBC]** If RFC 4301 is supported, the product shall be capable of disabling the BYPASS IPSec processing choice.

NOTE: The intent of this requirement is to ensure that no packets are transmitted unless they are protected by IPSec.

22.3 **[Required: EI (Softphone Only), R] [Conditional: EI, NA/SS, LS, EBC]** If RFC 4301 is supported, the product shall not support the mixing of IPv4 and IPv6 in a security association.

22.4 **[Required: EI (Softphone Only), R] [Conditional: EI, NA/SS, LS, EBC]** If RFC 4301 is supported, the product's security association database (SAD) cache shall have a method to uniquely identify a SAD entry. NOTE: The concern is that a single SAD entry will be associated with multiple security associations. RFC 4301, Section 4.4.2, describes a scenario where this could occur.

22.5 **[Required: EI (Softphone Only), R] [Conditional: EI, NA/SS, LS, EBC]** If RFC 4301 is supported, the product shall be capable of correlating the DSCP for a VVoIP stream to the security association in accordance with Section 5.3.2, Assured Services Requirements and Section 5.3.3, Network Infrastructure E2E Performance Requirements, plain text DSCP plan.

22.6 **[Required: EI (Softphone Only), R] [Conditional: EI, NA/SS, LS, EBC]** If RFC 4301 is supported, the product shall implement IPSec to operate with both integrity and confidentiality.

22.7 **[Required: EI (Softphone Only, R)] [Conditional: EI, NA/SS, LS, EBC]** If RFC 4301 is supported, the product shall be capable of enabling and disabling the ability of the product to send an ICMP message informing the sender that an outbound packet was discarded.

22.7.1 **[Required: EI (Softphone Only), R] [Conditional: EI, NA/SS, LS, EBC]** If an ICMP outbound packet message is allowed, the product shall be capable of rate limiting the transmission of ICMP responses.

22.8 **[Required: EI (Softphone Only), R] [Conditional: EI, NA/SS, LS, EBC**] If RFC 4301 is supported, the product shall be capable of enabling or disabling the propagation of the Explicit Congestion Notification (ECN) bits.

22.9 **[Required: EI (Softphone Only), R] [Conditional: EI, NA/SS, LS, EBC]** If RFC 4301 is supported, the system's Security Policy Database (SPD) shall have a nominal, final entry that discards anything unmatched.

22.10 **[Required: EI (Softphone Only), R] [Conditional: EI, NA/SS, LS, EBC]** **[Alarm]** If RFC 4301 is supported, and the product receives a packet that does not match any SPD cache entries and the product determines it should be discarded, the product shall log the event and include the date/time, Security Parameter Index (SPI) if available, IPSec protocol if available, source and destination of the packet, and any other selector values of the packet.

NOTE: Some products may not be able to log all this information (e.g., the product may not have access to this information).

22.11 **[Required: EI (Softphone Only), R] [Conditional: EI, NA/SS, LS, EBC]** **[Alarm]** If RFC 4301 is supported, the product should include a management control to allow an administrator to enable or disable the ability of the product to send an Internet Key Exchange (IKE) notification of an INVALID_SELECTORS.

NOTE: Some products may not be able to log all this information (e.g., the product may not have access to this information).

22.12 **[Required: EI (Softphone Only), R] [Conditional: EI, NA/SS, LS, EBC]** If RFC 4301 is supported, the product shall support the Encapsulating Security Payload (ESP) Protocol in accordance with RFC 4303.

22.12.1 **[Required: EI (Softphone Only), R] [Conditional: EI, NA/SS, LS, EBC]** If RFC 4303 is supported, the product shall be capable of enabling anti-replay.

22.12.2 **[Required: EI (Softphone Only), R] [Conditional: EI, NA/SS, LS, EBC]** If RFC 4303 is supported, the product shall check, as its first check, after a packet has been matched to its SA whether the packet contains a sequence number that does not duplicate the sequence number of any other packet received during the life of the security association.

22.13. **[Required: EI (Softphone Only), R] [Conditional: EI, NA/SS, LS, EBC]** If RFC 4301 is supported, the product shall support the cryptographic algorithms as defined in RFC 4308 for Suite Virtual Private Network (VPN)-B.

22.13.1. **[Required: EI (Softphone Only), R] [Conditional: EI, NA/SS, LS, EBC]** If RFC 4301 is supported, the product shall support the use of AES-CBC with 128-bits keys for encryption.

22.13.2. **[Required: EI (Softphone Only), R] [Conditional: EI, NA/SS, LS, EBC]** If RFC 4301 is supported, the product shall support the use of HMAC-SHA1-96 for (Threshold) and AES-XCBC-MAC-96 ~~(UCR 2010)~~.

22.14. **[Required: EI (Softphone Only), R] [Conditional: EI, NA/SS, LS, EBC]** If RFC 4301 is supported, the product shall support IKE version 1 (IKEv1) (Threshold) as defined in RFC 2409, and IKE version 2 (IKEv2) (UCR 2012~~0~~) as defined in RFC 4306 (UCR 2012~~0~~).

NOTE 1: The IKEv1 requirements are found in Section 5.4, Information Assurance.

NOTE 2: Even if IKEv2 is implemented, IKEv1 needs to be implemented as well for backwards compatibility.

22.14.1. **[Conditional: EI, NA/SS, R, LS, EBC]** If the product supports IKEv2, it shall be capable of configuring the maximum User Datagram Protocol (UDP) message size.

22.14.2 Reserved.

22.14.3 **[Conditional: EI, NA/SS, R, LS, EBC]** To prevent a DoS attack on the initiator of an IKE_SA, the initiator shall accept multiple responses to its first message, treat each as potentially legitimate, respond to it, and then discard all the invalid half-open connections when it receives a valid cryptographically protected response to any one of its requests. Once a cryptographically valid response is received, all subsequent responses shall be ignored whether or not they are cryptographically valid.

22.14.4 Reserved.

22.14.5 **[Conditional: EI, NA/SS, R, LS, EBC]** If the product supports IKEv2, the product shall reject initial IKE messages unless they contain a Notify Payload of type COOKIE.

22.14.6 **[Conditional: EI, NA/SS, R, LS, EBC]** If the product supports IKEv2, the product shall close an SA instead of rekeying when its lifetime expires if there has been no traffic since the last rekey.

22.14.7 **[Conditional: EI, NA/SS, R, LS, EBC]** If the product supports IKEv2, the product shall not use the Extensible Authentication Protocol (EAP) method for IKE authentication.

22.14.8 **[Conditional: EI, NA/SS, R, LS, EBC]** If the product supports IKEv2, the product shall limit the frequency to which it responds to messages on UDP port 500 or 4500 when outside the context of a security association known to it.

22.14.9 **[Conditional: EI, NA/SS, R, LS, EBC]** If the product supports IKEv2, the product shall not support temporary IP addresses or respond to such requests.

22.14.10 **[Conditional: EI, NA/SS, R, LS, EBC]** If the product supports IKEv2, the product shall support the IKEv2 cryptographic algorithms defined in RFC 4307.

22.14.11 **[Conditional: EI, NA/SS, R, LS, EBC]** If the product supports IKEv2, the product shall support the VPN-B Suite as defined in RFC 4308 ~~and RFC 4869~~ (UCR 2012~~0~~).

- Encryption – AES with 128-bit keys in CBC Mode
- Pseudo-random function – AES-XCBC-PRF-128
- Integrity – AES-XCBC-MAC-96
- Diffie-Hellman Group – 2048-bit MODP
- Rekeying of Phase 2 or the CREATE_CHILD_SA shall be supported by both parties. The initiator of the exchange may include a Diffie-Hellman key; if included, it shall be a type 2048 – bit MODP. If the initiator of the exchange includes a Diffie-Hellman key, the responder shall include a Diffie-Hellman key and it shall also be a type 2048-bit MODP.

22.14.12 **Conditional: EI, NA/SS, R, LS, EBC]** If the product supports IKEv2,

the product shall support the following VPN Suites as defined in RFC 4869 (UCR 2012):

- Suite-B-GCM-128
- Suite-B-GMAC-128

~~NOTE: RFC 4869 Suite B Cryptographic Suites for IPSec identifies four new cryptographic user interface suites based on implementations of the U.S. NSA's Suite B algorithms.~~

22.15 **[Required: EI (Softphone Only), R] [Conditional: EI, NA/SS, LS, EBC]** If RFC 4301 is supported, the product shall support extensions to the Internet IP Security Domain of Interpretation for the Internet Security Association and Key Management Protocol (ISAKMP) as defined in RFC 2407.

22.16 **[Required: EI (Softphone Only), R] [Conditional: EI, NA/SS, LS, EBC]** If RFC 4301 is supported, the product shall support the ISAKMP as defined in RFC 2408.

22.17 **[Required: R] [Conditional: EI, NA/SS, LS, EBC]** If the product supports the IPSec Authentication Header Mode, the product shall support the IP Authentication Header (AH) as defined in RFC 4302.

22.18 **[Required: EI (Softphone Only), R] [Conditional: EI, NA/SS, LS, EBC]** If RFC 4301 is supported, the product shall support manual keying of IPSec.

22.19 **[Required: EI (Softphone Only), R] [Conditional: EI, NA/SS, LS, EBC]** If RFC 4301 is supported, the product shall support the ESP and AH cryptographic algorithm implementation requirements as defined ~~in RFC 4305 and~~ RFC 4835

NOTE: RFC 4835 replace the now obsolete RFC 4305.~~(UCR 2010).~~

22.20 Reserved.

22.21 **[Required: EI (Softphone Only), R] [Conditional: EI, NA/SS, LS, EBC]** If RFC 4301 is supported, the product shall support the IKEv1 security algorithms as defined in RFC 4109.

5.3.5.4.10 Network Management

23. **[Conditional: R, LS]** If IPv6-compatible nodes are managed via SNMP, the product shall comply with the Management Information Base (MIB) for IPv6 textual conventions and general group as defined in RFC 4293.

    NOTE: The requirements to support SNMPv3 are found in Section 5.3.2.17.3.1.5, SNMP Version 2 and Version 3 Format Alarm messages, and Section 5.4, Information Assurance Requirements.

    NOTE: By calendar year (CY) 2011 nodes managed via SNMPv3 are required to do so using IPv6 transport.

    23.1 **[Conditional: R, LS]** If the product performs routing functions and if IPv6-capable nodes are managed via SNMP management, the product shall support the SNMPv3 management framework as described in RFC 3411.

    23.2 **[Conditional: R, LS]** If the product performs routing functions and if IPv6-capable nodes are managed via SNMP management, the product shall support SNMPv3 message processing and dispatching as described in RFC 3412.

    23.3 **[Conditional: R, LS]** If the product performs routing functions and if IPv6-capable nodes are managed via SNMP management, the product shall support the SNMPv3 applications as described in RFC 3413.

24. **[Conditional: R, LS]** If IPv6-compatible nodes are managed via SNMP, the product shall support the IP MIBs as defined in RFC 4293.

25. **[Conditional: R, LS]** If IPv6-compatible nodes are managed via SNMP, the product shall support the TCP MIBs as defined in RFC 4022.

26. **[Conditional: R, LS]** If IPv6-compatible nodes are managed via SNMP, the product shall support the UDP MIBs as defined in RFC 4113.

27. **[Conditional: R, LS]** If the product performs routing functions and tunneling functions, the product shall support IP tunnel MIBs as described in RFC 4087.

28. **[Conditional: R, LS]** If the product performs routing functions and is managed by SNMP, the product shall support the IP Forwarding MIB as defined in RFC 4292.

29. **[Conditional: R, LS]** If the product supports mobile users, the product shall support the Mobile IP Management MIBs as described in RFC 4295 (UCR 2012~~0~~).

30. Reserved.~~**[Conditional: R, LS]** If IPv6-capable Nodes are managed via SNMP implementation and support routing functions, the product shall support the textual conventions for IPv6 flow labels as described in RFC 3595.~~

31. **[Conditional: R, LS]** If the product supports routing functions and if the IPSec policy database is configured through SNMPv3, the product shall support RFC 4807.

32. **[Required: EI (Softphone only)] [Conditional: EI, NA/SS, R, LS, EBC]** If the product uses URIs, the product shall use the URI syntax described in RFC 3986.

    NOTE: According to "DoD IPv6 Standard Profiles For IPv6-capable Products-Supplemental Guidance" Version 4.0, RFC 3986 is not a testable requirement for host or server products and has been deleted from the product class requirements of that document.

33. **[Conditional: EI, NA/SS]** If the product uses the DNS resolver, the product shall conform to RFC 3596 for DNS queries.

    NOTE: DNS is primarily used for NM applications.

5.3.5.4.11 Traffic Engineering

34. **[Required: NA/SS, R, LS, EBC]** For traffic engineering purposes, the bandwidth required per voice subscriber is calculated to be 110.0 kbps (each direction) for each IPv6 call. This is based on G.711 (20 ms codec) with IP overhead (100 kbps) resulting in a 250 byte bearer packet plus 10 kbps for signaling, Ethernet Interframe Gap, and the SRTCP overhead. Based on overhead bits included in the bandwidth calculations, vendor implementations may use different calculations and hence arrive at slightly different numbers.

35. **[Required: R, LS]** The number of VoIP subscribers per link size for IPv6 is the same as for IPv4 and is defined in Section 5.3.1, Assured Services Local Area Network Infrastructure Product Requirements.

36. **[Required: R, LS]** The number of video subscribers per link size for IPv6 is the same as for IPv4 and is defined in Section 5.3.1, Assured Services Local Area Network Infrastructure.

5.3.5.4.12 IP Version Negotiation

37. **[Required: NA/SS, EBC]** The product shall forward packets using the same IP Version as the Version in the received packet.

NOTE: If the packet was received as an IPv6 packet, the appliance will forward it as an IPv6 packet. If the packet was received as an IPv4 packet, the appliance will forward the packet as an IPv4 packet. This requirement is primarily associated with the signaling packets to ensure that translation does not occur. This requirement may be waived from CY 2008 –CY 2012 to support IPv4 or IPv6 only EIs.

38. **[Required: EI, NA/SS]** The product shall use the Alternative Network Address Types (ANAT) semantics for the Session Description Protocol (SDP) in accordance with RFC 4091 when establishing media streams from dual-stacked appliances for AS-SIP signaled sessions.

    38.1 **[Required: EI, NA/SS]** The product shall prefer any IPv4 address to any IPv6 address when using ANAT semantics.

    NOTE: This requirement will result in all AS-SIP sessions being established using IPv4.

    38.2 **[Required: EI, NA/SS]** The product shall place the option tag "SDP-ANAT" in a Required header field when using ANAT semantics in accordance with RFC 4092.

    38.3 **[Required: EI]** Dual-stacked products shall include the IPv4 and IPv6 addresses within the SDP of the SIP INVITE message when the INVITE contains the SDP.

5.3.5.4.13 AS-SIP IPv6 Unique Requirements

39. **[Conditional: EI, NA/SS, EBC]** If the product is using AS-SIP and the <addrtype> is IPv6 and the <connection-address> is a unicast address, the product shall support generation and processing of unicast IPv6 addresses having the following formats:

    - x:x:x:x:x:x:x:x (where *x* is the hexadecimal values of the eight 16-bit pieces of the address). Example: 1080:0:0:0:8:800:200C:417A

    - x:x:x:x:x:x:d.d.d.d (where *x* is the hexadecimal values of the six high-order 16-bit pieces of the address, and *d* is the decimal values of the four low-order 8-bit pieces of the address (standard IPv4 representation). For example, 1080:0:0:0:8:800:116.23.135.22.

40. **[Conditional: EI, NA/SS, EBC]** If the product is using AS-SIP, the product shall support the generation and processing of IPv6 unicast addresses using compressed zeros consistent with one of the following formats:

- x:x:x:x:x:x:x:x format: 1080:0:0:0:8:800:200C:417A
- x:x:x:x:x:x:d.d.d.d format: 1080:0:0:0:8:800:116.23.135.22
- compressed zeros: 1080::8:800:200C:417A

41. **[Conditional: EI, NA/SS, EBC]** If the product is using AS-SIP and the <addrtype> is IPv6 and the <connection-address> is a multicast group address (i.e., the two most significant hexadecimal digits are FF), the product shall support the generation and processing of multicast IPv6 addresses having the same formats as the unicast IPv6 addresses.

42. **[Conditional: EI, NA/SS, EBC]** If the product is using AS-SIP and the <addrtype> is IPv6, the product shall support the use of ~~RFC 3266 and~~ RFC 4566 ~~[UCR 2010]~~ for IPv6 in SDP as described in Section 5.3.4, AS-SIP Requirements.

NOTE: RFC 4566 replaced the now obsolete RFC 3266.

43. **[Conditional: EI, NA/SS, EBC]** If the product is using AS-SIP and the <addrtype> is IPv6 and the <connection-address> is an IPv6 multicast group address, the multicast connection address shall not have a Time To Live (TTL) value appended to the address as IPv6 multicast does not use TTL scoping.

44. **[Conditional: EI, NA/SS, EBC]** If the product is using AS-SIP, the product shall support the processing of IPv6 multicast group addresses having the <number of address> field and may support generating the <number of address> field. This field has the identical format and operation as the IPv4 multicast group addresses.

45. **[Required: EBC]** The product shall be able to provide topology hiding (e.g., NAT) for IPv6 packets as described in Section 5.4, Information Assurance Requirements.

46. **[Required: EI (Softphone Only)]** The product shall support default address selection for IPv6 as defined in RFC 3484 (except for Section 2.1).

NOTE: It is assumed that an IPv6 appliance will have as a minimum an IPv6 link local and an IPv4 address, and will have at least two addresses.

5.3.5.4.14 Miscellaneous Requirements

47. **[Conditional: R, EBC]** If the product supports Remote Authentication Dial In User Service (RADIUS) authentication, the product shall support RADIUS as defined in RFC 3162.

[Conditional: LS] If the LS supports a routing function, the product shall support RFC 3162.

NOTE: RFC 3162 only defines the additional attributes of RADIUS that are unique to IPv6 implementations. For the base RADIUS requirements, other RFCs are required, such as RFC 2865.

NOTE: Because RFC 3162 cites the Network Access Server (NAS) functions would be on the Access Point (router), this function should be a feature of the router.

48. **[Conditional: EI (Softphone Only)]** If the product supports Mobile IP Version 6 (MIPv6), the product shall provide mobility support as defined in RFC 3775 (UCR 2012~~0~~).

    48.1. **[Conditional: R]** If the product acts as a home agent, the product shall provide mobility support as defined in RFC 3775 (UCR 2012~~0~~).

49. **[Conditional: EI (Softphone Only), R]** If the product supports MIPv6, the product shall provide a secure manner to signal between mobile nodes and home agents as described in RFC 3776 (UCR 2012~~0~~) and RFC 4877 (UCR 2012~~0~~).

50. ~~—~~ **[Conditional: R]** If the product is used in an IPv6 mobility application, the product shall use RFC 4429 Optimistic Duplicate Address Detection (DAD) (UCR 2012) in lieu of a standard DAD. (Guidance based upon results from recommendations from JUICE 2010.) Further, to mitigate the "Man-in-the-middle" attack for neighbor discovery, the network must use RFC 3971 Secure Neighbor Discovery (SEND) or equivalent (UCR 2012).
~~Reserved.~~

51. **[Conditional: R]** If the product supports network mobility (NEMO), the product shall support the function as defined in RFC 3963 (UCR 2012~~0~~).

52. **[Required: EI, NA/SS, R, EBC]** The products shall support Differentiated Services as described in RFC 2474 for a voice and video stream in accordance with Section 5.3.2, Assured Services Requirements, and Section 5.3.3, Network Infrastructure E2E Performance Requirements, plain text DSCP plan.

    52.1 **[Conditional: LS]** If the LS supports a routing function, the product shall support RFC 2474.

    52.2 **[Required: R, LS]** The product shall support RFC 3168 for the incorporation of Explicit Congestion Notification (ECN) to TCP and IP, including ECN's use of two bits in the IP header.

NOTE: This applies to The Core, Distribution, and Access products as identified in Section 5.3.1.3.5 Protocols.

53. **[Conditional: EI (Softphone Only), R]** If the product acts as an IPv6 tunnel broker, the product shall support the function as defined in RFC 3053.

54. **[Conditional: R]** If the product supports roaming (as defined within RFC 4282), the product shall support this function as described by RFC 4282.

55. **[Conditional: R]** If the product supports the Point-to-Point Protocol (PPP), the product shall support PPP as described in ~~RFC 2472 and~~ RFC 5072 ~~(UCR 2010)~~.

NOTE: RFC 5072 replaced the now obsolete RFC 2472.

56 **[Required: LS] [Conditional: R]** To support ASLAN assured services, all LAN switches that provide layer 3 functionality to the access layer shall support Virtual Router Redundancy protocol (VRRP) for IPv6 as detailed in RFC 5798.

NOTE: This applies to products only in the AS LAN.

57. **[Required: NA/SS, R, LS]** The product shall support RFC 4330 Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI (UCR 2012).

58. As noted in DoD IPv6 Standard Profiles Version 5.0, Robust Header Compression (RoHC) is designed to provide a significant improvement in transmission efficiency for bandwidth limited networks. It will likely be used in cellular networks (2.5G, 3G and 4G) and other wireless links. Because it is an emerging technology, the following RFCs will be reviewed for possible inclusion in UCR 2012 as **[Conditional: EI, NA/SS, R, LS]**:

- RFC 3095, RObust Header Compression (ROHC) – Supports reliable IP header compression over wireless links. RFC 4815, Corrections and Clarifications to RFC 3095.
- RFC 5795 RoHC Framework – Provides an unmodified extract of the framework definition from RFC 3095.
- RFC 4996, RObust Header Compression (ROHC): A Profile for TCP/IP (ROHC-TCP) – Provides a specific profile for compression of TCP/IP headers based on the framework defined in RFC 5795.
- RFC 3241, RObust Header Compression (ROHC) over PPP– Provides for compression over various PPP and low-speed links.
- RFC 3843, RObust Header Compression (ROHC): A Compression Profile for IP– Provides additional guidance for extending RFC 3095 for any arbitrary IP header chain for reliable IP header compression over wireless links.

- RFC 4362, RObust Header Compression (ROHC): A Link-Layer Assisted Profile for IP/UDP/RTP– Provides additional guidance for optimizing RFC 3095 for various link-layers and supports reliable IP header compression over wireless links.

59. As noted in DoD IPv6 Standard Profiles Version 5.0, IP Header Compression is an earlier alternative to RoHC for low-speed serial links requiring compression. Because it is an emerging technology, the following RFCs will be reviewed for possible inclusion in UCR 2012 as **[Conditional: EI, NA/SS, R, LS]**:

- RFC 2507, IP Header Compression - Describes how to compress multiple IP headers and TCP and UDP headers per hop over point to point links.
- RFC 2508, Compressing IP/UDP/RTP Headers for Low-Speed Serial Links - Describes a method for compressing the headers of IP/UDP/RTP datagrams to reduce overhead on low-speed serial links.
- RFC 3173, IP Payload Compression - Describes a protocol intended to provide lossless compression for Internet Protocol datagrams in an Internet environment.

60. As noted in DoD IPv6 Standard Profiles Version 5.0, multicast routing protocols have emerged from the IETF Protocol Independent Multicast (PIM) Working Group as Proposed Standards. Because it is an emerging technology, the following RFCs will be reviewed for possible inclusion in UCR 2012 as **[Conditional: R]**:

- RFC 5110 Overview of the Internet Multicast Routing Architecture - Describes multicast routing architectures that are currently deployed on the Internet.
- RFC 4601, Protocol Independent Multicast – Sparse Mode (PIM-SM) – Specifies PIM-SM which is a multicast routing protocol that can use the underlying unicast routing information base or a separate multicast- capable routing information base.
- RFC 3973, Protocol Independent Multicast – Dense Mode (PIM-DM) Specifies PIM-DM which is a multicast routing protocol that uses the underlying unicast routing information base to flood multicast datagrams to all multicast routers.

NOTE: DoD IPv6 Standard Profile Version 5.0 states that RFC 3973 is currently Experimental and not widely implemented, but may be considered for optional use where appropriate.

5.3.5.5 Mapping of RFCs to UC Profile Categories

~~In Section 5.3.5.1, Introduction, the DoD IPv6 Profile, Version 3.0, five exceptions are listed. Tables 5.3.5.2 through 5.3.5.6 identify these exceptions with an asterisk (*[n]), where *n* is one of the five exceptions.~~

Table 5.3.5-2. UC Host/Workstation (EI (Softphone))

RFC NUMBER	RFC TITLE	REQUIRED – R ** CONDITIONAL – C
1981	Path MTU Discovery for IP Version 6	R-8
~~2401~~	~~Security Architecture for the Internet Protocol~~	~~R-8; C~~
2407	The Internet IP Security Domain of Interpretation for ISAKMP	R-8; C
2408	Internet Security Association and Key Management Protocol (ISAKMP)	R-8; C
2409	The Internet Key Exchange (IKE)	R-8; C
2460	Internet Protocol, Version 6 (IPv6) Specification	R-2
~~2461~~	~~Neighbor Discovery for IP Version 6 (IPv6)~~	~~R~~
~~2462~~	~~IPv6 Stateless Address Autoconfiguration~~	~~C~~
2464	Transmission of IPv6 Packets over Ethernet Networks	R-3
2474	Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers	R~~*~~(3)-4
2710	Multicast Listener Discovery (MLD) for IPv6	R-8; R
2711	IPv6 Router Alert Option	R~~*~~(1)-8
~~3041~~	~~Privacy Extensions for Stateless Address Autoconfiguration in IPv6~~	~~C-8~~
3053	IPv6 Tunnel Broker	C~~*~~(3)-8
~~3266~~	~~Support for IPv6 in Session Description Protocol (SDP)~~	~~C*(4)~~
3315	Dynamic Host Configuration Protocol for IPv6 (DHCPv6)	C
3484	Default Address Selection for Internet Protocol Version 6 (IPv6)	R~~*~~(3)-8
3596	DNS Extensions to Support IPv6	C~~*~~(3)
3775	Mobility Support in IPv6	C-8, C-12~~0~~
3776	Using IPSec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents	C-8, C-12~~0~~
3810	Multicast Listener Discovery Version 2 (MLDv2) for IPv6	R-8
3986	Uniform Resource Identifier (URI): Generic Syntax	R~~*~~(2)-8; C~~*~~(2)
4007	IPv6 Scoped Address Architecture	R
4091	The Alternative Network Address Types (ANAT) Semantics for the Session Description Protocol (SDP) Grouping Framework	R~~*~~(4)
4092	Usage of the Session Description Protocol (SDP) Alternative Network Address Types (ANAT) Semantics in the Session Initiation Protocol (SIP)	R~~*~~(4)
4109	Algorithms for Internet Key Exchange Version 1 (IKEv1)	R-8; C
4213	Basic Transition Mechanisms for IPv6 Hosts and Routers	C -1
4291	IP Version 6 Addressing Architecture	R
4301	Security Architecture for the Internet Protocol	R-8~~, R-10~~; C~~-10~~
4302	IP Authentication Header	C~~*~~(3)
4303	IP Encapsulating Security Payload (ESP)	R-8; C
~~4305~~	~~Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)~~	~~R-8; C~~
4306	Internet Key Exchange (IKEv2) Protocol	R-8, R-12~~0~~; C-12~~0~~

RFC NUMBER	RFC TITLE	REQUIRED – R ** CONDITIONAL – C
4307	Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2)	C
4308	Cryptographic Suites for IPSec	R~~*(1)~~-8, C*(1)
4443	Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification	R
4566	SDP: Session Description Protocol	C~~*(4) 10~~
4835	Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)	R-8, C~~R-10; C-10~~
4861	Neighbor Discovery for IP Version 6 (IPv6)	R~~-10~~
4862	IPv6 Stateless Address Autoconfiguration	~~C-10~~R
4869	Suite B Cryptographic Suites for IPSec	C-12~~0~~
4877	Mobile IPv6 Operation with IKEv2 and the Revised IPSec Architecture	C-8, C-12~~0~~
4941	Privacy Extensions for Stateless Address Autoconfiguration in IPv6	C-8~~, C-10~~
5095	Deprecation of Type 0 Routing Headers in IPv6	R~~*(1)~~

~~NOTES:~~
~~C/R-1: Only meets the dual-stack requirements of this RFC.~~
~~R-2: Only meets IPv6 formatting requirements of this RFC.~~
~~R-3: Only meets framing format aspects of RFC.~~
~~R-4: Requirement covered in Section 5.3.3, Wide Area Network General System Requirements~~
~~C-5: Condition is that product acts as a router.~~
~~C-6: Only applies to MGs.~~
~~C-7: Requirements only apply if the product acts as an edge router.~~
~~C/R-8: EI (softphones only).~~
~~C/R-10: Conditional/Objective Requirement for UCR 2010.~~
~~*(n): Deviation from DoD IPv6 Profile, Version 3.0, Appendix C. Key to "n" values is described in Section 5.3.5.1, Introduction.~~

NOTES:
C/R-1: Only meets the dual-stack requirements of this RFC.
C/R-2: Only meets IPv6 formatting requirements of this RFC.
R-3: Only meets framing format aspects of RFC.
R-4: Requirement covered in Section 5.3.3, Wide Area Network General System Requirements.
C-5: Condition is that product acts as a router.
C-6: Only applies to MGs.
C-7: Requirements only apply if the product acts as an edge router.
C/R-8: EI (softphones only).
C/R-12: Conditional/Objective Requirement for UCR 2012.
* Deviation from DoD IPv6 Profile, version 5.0, Appendix C.
** This column can have (1) softphones only, e.g. R-8, (2) EI, e.g. R-3; or (3) Softphones only and EI, e.g. R-8; C.

Table 5.3.5-3. UC Simple Server (LSC, MFSS)/ UC Network Appliance (MG)

RFC NUMBER	RFC TITLE	REQUIRED – R CONDITIONAL – C
~~2401~~	~~Security Architecture for the Internet Protocol~~	~~C*(3)~~

RFC NUMBER	RFC TITLE	REQUIRED – R CONDITIONAL – C
2407	The Internet IP Security Domain of Interpretation for ISAKMP	C~~*(3)~~
2408	Internet Security Association and Key Management Protocol (ISAKMP)	C~~*(3)~~
2409	The Internet Key Exchange (IKE)	C~~*(3)~~
2460	Internet Protocol, Version 6 (IPv6) Specification	R-2
~~2461~~	~~Neighbor Discovery for IP Version 6 (IPv6)~~	~~R~~
~~2462~~	~~IPv6 Stateless Address Autoconfiguration~~	~~C~~
2464	Transmission of IPv6 Packets over Ethernet Networks	R-3
2474	Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers	R~~*(3)~~-4
2710	Multicast Listener Discovery (MLD) for IPv6	R
~~3266~~	~~Support for IPv6 in Session Description Protocol (SDP)~~	~~C*(4)~~
3315	Dynamic Host Configuration Protocol for IPv6 (DHCPv6)	C
3596	DNS Extensions to Support IPv6	C~~*(3)~~
3986	Uniform Resource Identifier (URI): Generic Syntax	C~~*(2)~~
4007	IPv6 Scoped Address Architecture	R
4091	The Alternative Network Address Types (ANAT) Semantics for the Session Description Protocol (SDP) Grouping Framework	R~~*(4)~~
4092	Usage of the Session Description Protocol (SDP) Alternative Network Address Types (ANAT) Semantics in the Session Initiation Protocol (SIP)	R~~*(4)~~
4109	Algorithms for Internet Key Exchange Version 1 (IKEv1)	C~~*(3)~~
4213	Basic Transition Mechanisms for IPv6 Hosts and Routers	R-1
4291	IP Version 6 Addressing Architecture	R
4301	Security Architecture for the Internet Protocol	C~~*(3)~~ ~~-10~~
4302	IP Authentication Header	C~~*(3)~~
4303	IP Encapsulating Security Payload (ESP)	C~~*(3)~~
~~4305~~	~~Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)~~	~~C*(3)~~
4306	Internet Key Exchange (IKEv2) Protocol	C~~*(3)~~-12~~0~~
4307	Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2)	C~~*(3)~~
4308	Cryptographic Suites for IPSec	C~~*(1, 3)~~
4330	Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI	R*-12
4443	Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification	R
4566	SDP: Session Description Protocol	C~~*(4)~~ ~~-10~~
4835	Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)	C ~~*(3)~~ ~~-10~~
4861	Neighbor Discovery for IP Version 6 (IPv6)	R ~~-10~~

RFC NUMBER	RFC TITLE	REQUIRED – R CONDITIONAL – C
4862	IPv6 Stateless Address Autoconfiguration	~~C-10~~R
4869	Suite B Cryptographic Suites for IPSec	C~~*(3)~~-12~~0~~
5095	Deprecation of Type 0 Routing Headers in IPv6	R~~*(1)~~

~~NOTES:~~
~~R-1: Only meets the dual-stack requirements of this RFC.~~
~~R-2: Only meets IPv6 formatting requirements of this RFC.~~
~~R-3: Only meets framing format aspects of RFC.~~
~~R-4: Requirement covered in Section 5.3.3, Wide Area Network General System Requirements.~~
~~C-5: Condition is that product acts as a router.~~
~~C-6: Only applies to MGs.~~
~~C-7: Requirements only apply if the product acts as an edge router.~~
~~C/R-8: EI (softphones only).~~
~~C/R-10: Conditional/Objective Requirement for UCR 2010.~~
~~*(n): Deviation from DoD IPv6 Profile, version 3.0, Appendix C. Key to "n" values is described in Section 5.3.5.1, Introduction~~ NOTES:
C/R-1: Only meets the dual-stack requirements of this RFC.
C/R-2: Only meets IPv6 formatting requirements of this RFC.
R-3: Only meets framing format aspects of RFC.
R-4: Requirement covered in Section 5.3.3, Wide Area Network General System Requirements.
C-5: Condition is that product acts as a router.
C-6: Only applies to MGs.
C-7: Requirements only apply if the product acts as an edge router.
C/R-8: EI (softphones only).
C/R-12: Conditional/Objective Requirement for UCR 2012.
* Deviation from DoD IPv6 Profile, version 5.0, Appendix C.~~.~~

Table 5.3.5-4. UC Router (R)

RFC NUMBER	RFC TITLE	REQUIRED – R CONDITIONAL – C
1772	Application of the Border Gateway Protocol in the Internet	C-7
1981	Path MTU Discovery for IPv6	R
~~2401~~	~~Security Architecture for the Internet Protocol~~	~~R~~
2404	The Use of HMAC-SHA-1-96 within ESP and AH	R
2407	The Internet IP Security Domain of Interpretation for ISAKMP	R
2408	Internet Security Association and Key Management Protocol (ISAKMP)	R
2409	The Internet Key Exchange (IKE)	R
2460	Internet Protocol, Version 6 (v6) Specification	R-2
~~2461~~	~~Neighbor Discovery for IP Version 6 (IPv6)~~	~~R~~
~~2462~~	~~IPv6 Stateless Address Autoconfiguration~~	~~C~~
2464	Transmission of IPv6 Packets over Ethernet Networks	R-3
~~2472~~	~~IP Version 6 over PPP~~	~~C~~
2473	Generic Packet Tunneling in IPv6 Specification	C-7
2474	Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers	R-4

RFC NUMBER	RFC TITLE	REQUIRED – R CONDITIONAL – C
2545	Use of BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing	C-7
2710	Multicast Listener Discovery (MLD) for IPv6	R
2711	IPv6 Router Alert Option	R*(1)
~~2740~~	~~OSPF for IPv6~~	~~R~~
2784	Generic Router Encapsulation (GRE)	C-7
~~2858~~	~~Multiprotocol Extensions for BGP-4~~	~~C-7~~
3053	IPv6 Tunnel Broker	C
3162	RADIUS and IPv6	C*(3)
3168	The Addition of Explicit Congestion Notification (ECN) to IP	R
3315	Dynamic Host Configuration Protocol for IPv6 (DHCPv6)	C
3411	An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks	C
3412	Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)	C
3413	Simple Network Management Protocol (SNMP) Applications	C
~~3595~~	~~Textual Conventions for IPv6 Flow Label~~	~~C~~
3775	Mobility Support in IPv6	C*(3)-120
3776	Using IPSec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents	C-120
3810	Multicast Listener Discovery Version 2 (MLDv2) for IPv6	R
3963	Network Mobility (NEMO) Basic Support Protocol	C-10
3971	SEcure Neighbor Discovery (SEND)	C-12
3986	Uniform Resource Identifier (URI): Generic Syntax	C*(2)
4007	IPv6 Scoped Address Architecture	R
4022	Management Information Base for the Transmission Control Protocol (TCP)	C
4087	IP Tunnel MIB	C*(3)
4109	Algorithms for Internet Key Exchange Version 1 (IKEv1)	R
4113	Management Information Base for the User Datagram Protocol (UDP)	C
4213	Basic Transition Mechanisms for IPv6 Hosts and Routers	R-1
4271	A Border Gateway Protocol 4 (BGP-4)	C-7
4282	The Network Access Identifier	C*(3)
4291	IP Version 6 Addressing Architecture	R
4292	IP Forwarding MIB	C
4293	Management Information Base for the Internet Protocol (IP)	C
4295	Mobile IP Management MIB	C-120
4301	Security Architecture for the Internet Protocol	R-10
4302	IP Authentication Header	R
4303	IP Encapsulating Security Payload (ESP)	R

RFC NUMBER	RFC TITLE	REQUIRED – R CONDITIONAL – C
~~4305~~	~~Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)~~	~~R~~
4306	Internet Key Exchange (IKEv2) Protocol	R-12~~0~~
4307	Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2)	C
4308	Cryptographic Suites for IPSec	R*(1)
4330	Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI	R*-12
4429	Optimistic Duplicate Address Detection (DAD) for IPv6	C-12
4443	Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification	R
4552	Authentication Confidentiality for OSPFv3	R
4760	Multiprotocol Extensions for BGP-4	C-7, C-~~10~~
4807	IPSec Security Policy Database Configuration MIB	C
4835	Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)	R-~~10~~
4861	Neighbor Discovery for IP Version 6 (IPv6)	R-~~10~~
4862	IPv6 Stateless Address Autoconfiguration	~~C-10~~R
4869	Suite B Cryptographic Suites for IPSec	C-12~~0~~
4877	MIPv6 Operation with IKE2 and the Revised IPSec Architecture	C-12~~0~~
5072	IP Version 6 over PPP	C-~~10~~
5095	Deprecation of Type 0 Routing Headers in IPv6	R~~*~~(1)
5304	IS-IS Cryptographic Authentication	R-~~10~~
5308	Routing IPv6 with ISIS	R-~~10~~
5310	IS-IS Generic Cryptographic Authentication	R-~~10~~
5798	Virtual Router Redundancy Protocol (VRRP) Version 3 for IPv4 and IPv6	C
5838	RFC 5838 Support of Address Families in OSPFv3	C-12

RFC NUMBER	RFC TITLE	REQUIRED – R CONDITIONAL – C
NOTES: C/R-1: Only meets the dual-stack requirements of this RFC. C/R-2: Only meets IPv6 formatting requirements of this RFC. R-3: Only meets framing format aspects of RFC. R-4: Requirement covered in Section 5.3.3, Wide Area Network General System Requirements. C-5: Condition is that product acts as a router. C-6: Only applies to MGs. C-7: Requirements only apply if the product acts as an edge router. C/R-8: EI (softphones only). C/R-12: Conditional/Objective Requirement for UCR 2012. * Deviation from DoD IPv6 Profile, version 5.0, Appendix C. ~~NOTES:~~ ~~R-1: Only meets the dual-stack requirements of this RFC.~~ ~~R-2: Only meets IPv6 formatting requirements of this RFC.~~ ~~R-3: Only meets framing format aspects of RFC.~~ ~~R-4: Requirement covered in Section 5.3.3, Wide Area Network General System Requirements.~~ ~~C-5: Condition is that product acts as a router.~~ ~~C-6: Only applies to MGs.~~ ~~C-7: Requirements only apply if the product acts as an edge router.~~ ~~C/R-8: EI (softphones only).~~ ~~C/R-10: Conditional/Objective Requirement for UCR 2010.~~ ~~*[n]: Deviation from DoD IPv6 Profile, version 3.0, Appendix C. Key to "n" values is described in Section 5.3.5.1, Introduction.~~		

Table 5.3.5-5. LAN Switch (LS)

RFC NUMBER	RFC TITLE	REQUIRED – R CONDITIONAL – C
Part 1 LAN Access Switch		
2407	The Internet IP Security Domain of Interpretation for ISAKMP	C
2408	Internet Security Association and Key Management Protocol (ISAKMP)	C
2409	The Internet Key Exchange (IKE)	C
2460	Internet Protocol, Version 6 (v6) Specification	C-2
2464	Transmission of IPv6 Packets over Ethernet Networks	R-3
2474	Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers	R-4
3168	The Addition of Explicit Congestion Notification (ECN) to IP	R
3411	An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks Note: SNMP "Over IPv6" requirement effective UCR 2012.	R
3412	Message Processing and Dispatching for the Simple Network Management Protocol (SNMP).	R
3413	Simple Network Management Protocol (SNMP) Applications Note: SNMP "Over IPv6" requirement effective UCR 2012.	R .
3644	Policy Quality of Service (QoS) Information Model	R

RFC NUMBER	RFC TITLE	REQUIRED – R CONDITIONAL – C
3986	Uniform Resource Identifier (URI): Generic Syntax	C
4007	IPv6 Scoped Address Architecture	R
4022	Management Information Base for the Transmission Control Protocol (TCP)	C
4087	IP Tunnel MIB	C
4109	Algorithms for Internet Key Exchange Version 1 (IKEv1)	C
4113	Management Information Base for the User Datagram Protocol (UDP)	C
4291	IP Version 6 Addressing Architecture	R
4292	IP Forwarding MIB	C
4293	Management Information Base for the Internet Protocol (IP)	C
4295	Mobile IP Management MIB	C-12
4301	Security Architecture for the Internet Protocol	C
4302	IP Authentication Header	C
4303	IP Encapsulating Security Payload (ESP)	C
4306	Internet Key Exchange (IKEv2) Protocol	C-12
4307	Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2)	C
4330	Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI	R*-12
4443	Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification	R
4807	IPSec Security Policy Database Configuration MIB	C
4835	Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)	C
4862	IPv6 Stateless Address Autoconfiguration	C
4869	Suite B Cryptographic Suites for IPSec	C-12
5095	Deprecation of Type 0 Routing Headers in IPv6	C
5798	Virtual Router Redundancy Protocol (VRRP) Version 3 for IPv4 and IPv6	R
Part 2 L3 Switch Requirements from Part 1 above, plus the below		
1981	Path MTU Discovery for IPv6	C-5
2404	The Use of HMAC-SHA-1-96 within ESP and AH	C-5
2710	Multicast Listener Discovery (MLD) for IPv6	C-5
2711	IPv6 Router Alert Option	C-5
3162	RADIUS and IPv6	C-5
3315	Dynamic Host Configuration Protocol for IPv6 (DHCPv6)	C-5
3411	An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks	C-5
3412	Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)	C-5
3413	Simple Network Management Protocol (SNMP) Applications	C-5
3810	Multicast Listener Discovery Version 2 (MLDv2) for IPv6	C-5

RFC NUMBER	RFC TITLE	REQUIRED – R CONDITIONAL – C
4213	Basic Transition Mechanisms for IPv6 Hosts and Routers	C-1, C-5
4552	Authentication Confidentiality for OSPFv3 (Routing protocol authentication only.)	C-5
4861	Neighbor Discovery for IP Version 6 (IPv6)	C-5
5304	IS-IS Cryptographic Authentication	C-5
5308	Routing IPv6 with ISIS	C-5
5310	IS-IS Generic Cryptographic Authentication	C-5
5798	Virtual Router Redundancy Protocol (VRRP) Version 3 for IPv4 and IPv6	C-5
5838	RFC 5838 Support of Address Families in OSPFv3	C-12
Part 3 L3 Switch (Edge Router) Requirements from Part 2 above, plus the below		
1772	Application of the Border Gateway Protocol in the Internet	C-5, C-7
2545	Use of BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing	C-5, C-7
4271	A Border Gateway Protocol 4 (BGP-4)	C-5, C-7
4760	Multiprotocol Extensions for BGP-4	C-5,C-7

NOTES:
C/R-1: Only meets the dual-stack requirements of this RFC.
C/R-2: Only meets IPv6 formatting requirements of this RFC.
R-3: Only meets framing format aspects of RFC.
R-4: Requirement covered in Section 5.3.3, Wide Area Network General System Requirements.
C-5: Condition is that product acts as a router.
C-6: Only applies to MGs.
C-7: Requirements only apply if the product acts as an edge router.
C/R-8: EI (softphones only).
C/R-12: Conditional/Objective Requirement for UCR 2012.
* Deviation from DoD IPv6 Profile, version 5.0, Appendix C.

~~RFC NUMBER~~	~~RFC TITLE~~	~~REQUIRED – R CONDITIONAL – C~~
~~1772~~	~~Application of the Border Gateway Protocol in the Internet~~	~~C-7~~
~~1981~~	~~Path MTU Discovery for IPv6~~	~~C-5~~
~~2401~~	~~Security Architecture for the Internet Protocol~~	~~C*(3)~~
~~2404~~	~~The Use of HMAC-SHA-1-96 within ESP and AH~~	~~C-5~~
~~2407~~	~~The Internet IP Security Domain of Interpretation for ISAKMP~~	~~C*(3)~~
~~2408~~	~~Internet Security Association and Key Management Protocol (ISAKMP)~~	~~C*(3)~~
~~2409~~	~~The Internet Key Exchange (IKE)~~	~~C*(3)~~
~~2460~~	~~Internet Protocol, Version 6 (v6) Specification~~	~~C-2, C-5~~
~~2461~~	~~Neighbor Discovery for IP Version 6 (IPv6)~~	~~C-5~~
~~2462~~	~~IPv6 Stateless Address Autoconfiguration~~	~~C~~
~~2464~~	~~Transmission of IPv6 Packets over Ethernet Networks~~	~~R-3~~

RFC NUMBER	RFC TITLE	REQUIRED – R CONDITIONAL – C
2474	Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers	C*(3) 4, C 5
2545	Use of BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing	C 7
2710	Multicast Listener Discovery (MLD) for IPv6	C 5
2711	IPv6 Router Alert Option	C*(1) 5
2740	OSPF for IPv6	C 5
2858	Multiprotocol Extensions for BGP-4	C 5, C 7
3162	RADIUS and IPv6	C*(3) 5
3315	Dynamic Host Configuration Protocol for IPv6 (DHCPv6)	C 5
3411	An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks	C 5
3412	Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)	C 5
3413	Simple Network Management Protocol (SNMP) Applications	C 5
3595	Textual Conventions for IPv6 Flow Label	C
3810	Multicast Listener Discovery Version 2 (MLDv2) for IPv6	C*(3) 5
3986	Uniform Resource Identifier (URI): Generic Syntax	C*(2)
4007	IPv6 Scoped Address Architecture	R
4022	Management Information Base for the Transmission Control Protocol (TCP)	C
4087	IP Tunnel MIB	C*(3)
4109	Algorithms for Internet Key Exchange Version 1 (IKEv1)	C*(3)
4113	Management Information Base for the User Datagram Protocol (UDP)	C
4213	Basic Transition Mechanisms for IPv6 Hosts and Routers	C 1, C 5
4271	A Border Gateway Protocol 4 (BGP-4)	C 7
4291	IP Version 6 Addressing Architecture	R
4292	IP Forwarding MIB	C
4293	Management Information Base for the Internet Protocol (IP)	C
4295	Mobile IP Management MIB	C 10
4301	Security Architecture for the Internet Protocol	C*(3) 10
4302	IP Authentication Header	C*(3)
4303	IP Encapsulating Security Payload (ESP)	C*(3)
4305	Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)	C*(3)
4306	Internet Key Exchange (IKEv2) Protocol	C*(3) 10
4307	Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2)	C*(3)
4308	Cryptographic Suites for IPSec	C*(1,3)
4443	Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification	C 5
4552	Authentication Confidentiality for OSPFv3	C 5
4760	Multiprotocol Extensions for BGP-4	C 5,C 7, C 10

~~RFC NUMBER~~	~~RFC TITLE~~	~~REQUIRED – R CONDITIONAL – C~~
~~4807~~	~~IPSec Security Policy Database Configuration MIB~~	~~C~~
~~4835~~	~~Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)~~	~~C*(3) 10~~
~~4861~~	~~Neighbor Discovery for IP Version 6 (IPv6)~~	~~C 5, C 10~~
~~4862~~	~~IPv6 Stateless Address Autoconfiguration~~	~~C 10~~
~~4869~~	~~Suite B Cryptographic Suites for IPSec~~	~~C*(3) 10~~
~~5095~~	~~Deprecation of Type 0 Routing Headers in IPv6~~	~~C*(1) 5~~
~~5304~~	~~IS-IS Cryptographic Authentication~~	~~C 5, C 10~~
~~5308~~	~~Routing IPv6 with ISIS~~	~~C 5, C 10~~
~~5310~~	~~IS-IS Generic Cryptographic Authentication~~	~~C 5, C 10~~

~~NOTES:~~
~~R 1: Only meets the dual-stack requirements of this RFC.~~
~~C/R 2: Only meets IPv6 formatting requirements of this RFC.~~
~~R 3: Only meets framing format aspects of RFC.~~
~~R 4: Requirement covered in Section 5.3.3, Wide Area Network General System Requirements.~~
~~C 5: Condition is that product acts as a router.~~
~~C 6: Only applies to MGs.~~
~~C 7: Requirements only apply if the product acts as an edge router.~~
~~C/R 8: EI (softphones only).~~
~~C/R 10: Conditional/Objective Requirement for UCR 2010.~~
~~*(n): Deviation from DoD IPv6 Profile, version 3.0, Appendix C. Key to "n" values is described in Section 5.3.5.1, Introduction.~~

Table 5.3.5-6. UC Information Assurance Device (EBC)

RFC NUMBER	RFC TITLE	REQUIRED – R CONDITIONAL – C
1981	Path MTU Discovery for IPv6	R
~~2401~~	~~Security Architecture for the Internet Protocol~~	~~C~~
2407	The Internet IP Security Domain of Interpretation for ISAKMP	C
2408	Internet Security Association and Key Management Protocol (ISAKMP)	C
2409	The Internet Key Exchange (IKE)	C
2460	Internet Protocol, Version 6 (v6) Specification	R-2
~~2461~~	~~Neighbor Discovery for IP Version 6 (IPv6)~~	~~R~~
~~2462~~	~~IPv6 Stateless Address Autoconfiguration~~	~~C~~
2464	Transmission of IPv6 Packets over Ethernet Networks	R-3
2474	Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers	R ~~*(3)~~-4
3162	RADIUS and IPv6	C ~~C*(3)~~
~~3266~~	~~Support for IPv6 in Session Description Protocol (SDP)~~	~~C*(4)~~
3986	Uniform Resource Identifier (URI): Generic Syntax	C~~*(2)~~
4007	IPv6 Scoped Address Architecture	R
4109	Algorithms for Internet Key Exchange Version 1 (IKEv1)	C

RFC NUMBER	RFC TITLE	REQUIRED – R CONDITIONAL – C
4213	Basic Transition Mechanisms for IPv6 Hosts and Routers	R-1
4291	IP Version 6 Addressing Architecture	R
4301	Security Architecture for the Internet Protocol	C~~-10~~
4302	IP Authentication Header	C*~~(3)~~
4303	IP Encapsulating Security Payload (ESP)	C
~~4305~~	~~Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)~~	~~C~~
4306	Internet Key Exchange (IKEv2) Protocol	C-12~~0~~
4307	Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2)	C
4308	Cryptographic Suites for IPSec	C*~~(1)~~
4443	Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification	R
4566	SDP: Session Description Protocol	C*~~(4)~~ ~~-10~~
4835	Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)	C~~-10~~
4861	Neighbor Discovery for IP version 6 (IPv6)	R~~-10~~
4862	IPv6 Stateless Address Autoconfiguration	~~C-10~~R
4869	Suite B Cryptographic Suites for IPSec	C-12~~0~~
5095	Deprecation of Type 0 Routing Headers in IPv6	R*~~(1)~~

NOTES:
C/R-1: Only meets the dual-stack requirements of this RFC.
C/R-2: Only meets IPv6 formatting requirements of this RFC.
R-3: Only meets framing format aspects of RFC.
R-4: Requirement covered in Section 5.3.3, Wide Area Network General System Requirements.
C-5: Condition is that product acts as a router.
C-6: Only applies to MGs.
C-7: Requirements only apply if the product acts as an edge router.
C/R-8: EI (softphones only).
C/R-12: Conditional/Objective Requirement for UCR 2012.
* Deviation from DoD IPv6 Profile, version 5.0, Appendix C. ~~NOTES:~~
~~R-1: Only meets the dual-stack requirements of this RFC.~~
~~R-2: Only meets IPv6 formatting requirements of this RFC.~~
~~R-3: Only meets framing format aspects of RFC.~~
~~R-4: Requirement covered in Section 5.3.3, Wide Area Network General System Requirements.~~
~~C-5: Condition is that product acts as a router.~~
~~C-6: Only applies to MGs.~~
~~C-7: Requirements only apply if the product acts as an edge router.~~
~~C/R-8: EI (softphones only).~~
~~C/R-10: Conditional/Objective Requirement for UCR 2010.~~
~~*(n): Deviation from DoD IPv6 Profile, version 3.0, Appendix C. Key to "n" values is described in Section 5.3.5.1, Introduction.~~

THIS PAGE INTENTIONALLY LEFT BLANK